National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 - 30 Jun 2020 Vol. 07 No. 12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
aapanel					
aapanel					
Argument Injection or Modification	18-06-2020	9	aaPanel through 6.6.6 allows remote authenticated users to execute arbitrary commands via the Script Content box on the Add Cron Job screen. **CVE ID : CVE-2020-14421**	N/A	A-AAP-AAPA-070820/1
Improper Input Validation	21-06-2020	6.5	aaPanel through 6.6.6 allows remote authenticated users to execute arbitrary commands via shell metacharacters in a modified /system?action=ServiceAdmin request (start, stop, or restart) to the setting menu of Sotfware Store. **CVE ID : CVE-2020-14950**	N/A	A-AAP-AAPA-070820/2
acf_to_rest_api_project					
acf_to_rest_api					
Information Exposure	24-06-2020	5	An issue was discovered in the acf-to-rest-api plugin through 3.1.0 for WordPress. It allows an insecure direct object reference via permalinks manipulation, as demonstrated by a wp-json/acf/v3/options/ request that reads sensitive information in the wp_options table, such as the	N/A	A-ACF-ACF_-070820/3

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			login and pass values. **CVE ID : CVE-2020-13700**		
Adobe					
character_animator					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-06-2020	9.3	Adobe Character Animator versions 3.2 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9586**	https://helpx.adobe.com/security/products/character_animator/apsb20-25.html	A-ADO-CHAR-070820/4
after_effects					
Out-of-bounds Read	26-06-2020	4.3	Adobe After Effects versions 17.0.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3809**	https://helpx.adobe.com/security/products/after_effects/apsb20-21.html	A-ADO-AFTE-070820/5
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9637**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	A-ADO-AFTE-070820/6
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9638**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	A-ADO-AFTE-070820/7
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have an out-of-bounds write	https://helpx.adobe.com/security	A-ADO-AFTE-070820/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9660**	/products/after_effects/apsb20-35.html	
Out-of-bounds Read	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9661**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	A-ADO-AFTE-070820/9
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9662**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	A-ADO-AFTE-070820/10
acrobat_dc					
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9592**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/11
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability.	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/12

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9593**		
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9594**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/13
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9595**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/14
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9596**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/15

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9597**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/16
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9598**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/17
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9599**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/18
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-070820/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9600**	b20-24.html	
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9601**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/20
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9602**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/21
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9603**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/22

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9604**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/23
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9605**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/24
Use After Free	25-06-2020	4.6	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9606**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/25
Use After Free	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb20-	A-ADO-ACRO-070820/26

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9607**	24.html	
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9608**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/27
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9609**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/28
NULL Pointer Dereference	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a null pointer vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9610**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9611**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/30
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9612**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/31
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9613**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/32
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb20-	A-ADO-ACRO-070820/33

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9614**	24.html	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	5.1	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a race condition vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9615**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/34
acrobat_reader_dc					
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9592**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/35
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/36

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9593		
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9594**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/37
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9595**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/38
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9596**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/39
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166	https://helpx.adobe.com/security/products/	A-ADO-ACRO-070820/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9597**	acrobat/apsb20-24.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9598**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/41
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9599**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/42
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2020-9600**		
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9601**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/44
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9602**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/45
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9603**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/46
Improper Restriction of Operations	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166	https://helpx.adobe.com/security/products/	A-ADO-ACRO-070820/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9604**	acrobat/apsb20-24.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9605**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/48
Use After Free	25-06-2020	4.6	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9606**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/49
Use After Free	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/50

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9607		
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9608**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/51
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9609**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/52
NULL Pointer Dereference	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a null pointer vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9610**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/53
Uncontrolled Resource Consumption	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and	https://helpx.adobe.com/security/products/acrobat/aps	A-ADO-ACRO-070820/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2015.006.30518 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9611**	b20-24.html	
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9612**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/55
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9613**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/56
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9614**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/57

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	5.1	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a race condition vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9615**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	A-ADO-ACRO-070820/58
coldfusion					
Improper Input Validation	26-06-2020	4.3	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an insufficient input validation vulnerability. Successful exploitation could lead to application-level denial-of-service (dos). **CVE ID : CVE-2020-3767**	https://helpx.adobe.com/security/products/coldfusion/apsb20-18.html	A-ADO-COLD-070820/59
Untrusted Search Path	26-06-2020	4.4	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have a dll search-order hijacking vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-3768**	https://helpx.adobe.com/security/products/coldfusion/apsb20-18.html	A-ADO-COLD-070820/60
Information Exposure	26-06-2020	4.3	ColdFusion versions ColdFusion 2016, and ColdFusion 2018 have an improper access control vulnerability. Successful exploitation could lead to system file structure disclosure. **CVE ID : CVE-2020-3796**	https://helpx.adobe.com/security/products/coldfusion/apsb20-18.html	A-ADO-COLD-070820/61

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
digital_editions					
Information Exposure	26-06-2020	4.3	Adobe Digital Editions versions 4.5.11.187212 and below have a file enumeration (host or local network) vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3798**	https://helpx.adobe.com/security/products/Digital-Editions/apsb20-23.html	A-ADO-DIGI-070820/62
premiere_pro					
Out-of-bounds Read	26-06-2020	4.3	Adobe Premiere Pro versions 14.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9616**	https://helpx.adobe.com/security/products/premiere_pro/apsb20-27.html	A-ADO-PREM-070820/63
Out-of-bounds Read	25-06-2020	9.3	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9652**	https://helpx.adobe.com/security/products/premiere_pro/apsb20-38.html	A-ADO-PREM-070820/64
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9653**	https://helpx.adobe.com/security/products/premiere_pro/apsb20-38.html	A-ADO-PREM-070820/65
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/premiere_pro/apsb20-	A-ADO-PREM-070820/66

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9654	38.html	
premiere_rush					
Out-of-bounds Read	26-06-2020	4.3	Adobe Premiere Rush versions 1.5.8 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9617**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-29.html	A-ADO-PREM-070820/67
Out-of-bounds Read	25-06-2020	9.3	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9655**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-39.html	A-ADO-PREM-070820/68
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9656**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-39.html	A-ADO-PREM-070820/69
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9657**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-39.html	A-ADO-PREM-070820/70
dng_software_development_kit					
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/dng-sdk/apsb20	A-ADO-DNG_-070820/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2020-9625**	-26.html	
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9627**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DNG_-070820/72
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9628**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DNG_-070820/73
campaign_classic					
Out-of-bounds Read	25-06-2020	4.3	Adobe Campaign Classic before 20.2 have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9666**	https://helpx.adobe.com/security/products/campaign/apsb20-34.html	A-ADO-CAMP-070820/74
bridge					
Information Exposure	26-06-2020	4.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9553**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/75
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write	https://helpx.adobe.com/security	A-ADO-BRID-070820/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9554**	/products/bridge/apsb20-19.html	
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9555**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/77
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9556**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/78
Out-of-bounds Read	26-06-2020	4.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9557**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/79
Out-of-bounds Read	26-06-2020	4.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9558**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/80
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/bridge/aps	A-ADO-BRID-070820/81

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2020-9559**	b20-19.html	
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9560**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/82
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9561**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/83
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9562**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/84
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9563**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/85
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9564**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9565**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/87
Use After Free	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9566**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/88
Use After Free	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9567**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/89
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9568**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/90
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9569**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	A-ADO-BRID-070820/91
illustrator					
Improper	26-06-2020	9.3	Adobe Illustrator versions	https://hel	A-ADO-ILLU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9570**	px.adobe.com/security/products/illustrator/apsb20-20.html	070820/92
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9571**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	A-ADO-ILLU-070820/93
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9572**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	A-ADO-ILLU-070820/94
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9573**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	A-ADO-ILLU-070820/95
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9574**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	A-ADO-ILLU-070820/96

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9575**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	A-ADO-ILLU-070820/97
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9639**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	A-ADO-ILLU-070820/98
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9640**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	A-ADO-ILLU-070820/99
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9641**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	A-ADO-ILLU-070820/100
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9642**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	A-ADO-ILLU-070820/101

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
digital_negative_software_development_kit					
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9589**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/102
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9590**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/103
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9620**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/104
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9621**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/105
Out-of-bounds Read	26-06-2020	4.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful	https://helpx.adobe.com/security/products/dng-	A-ADO-DIGI-070820/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to information disclosure. **CVE ID : CVE-2020-9622**	sdk/apsb20-26.html	
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9623**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/107
Out-of-bounds Read	26-06-2020	4.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9624**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/108
Out-of-bounds Read	26-06-2020	4.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9626**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/109
Out-of-bounds Read	26-06-2020	4.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9629**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	A-ADO-DIGI-070820/110
audition					
Out-of-	25-06-2020	4.3	Adobe Audition versions 13.0.5 and earlier have an	https://helpx.adobe.co	A-ADO-AUDI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9618**	m/security/products/audition/apsb20-28.html	070820/111
Out-of-bounds Write	25-06-2020	9.3	Adobe Audition versions 13.0.6 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9658**	https://helpx.adobe.com/security/products/audition/apsb20-40.html	A-ADO-AUDI-070820/112
Out-of-bounds Write	25-06-2020	9.3	Adobe Audition versions 13.0.6 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9659**	https://helpx.adobe.com/security/products/audition/apsb20-40.html	A-ADO-AUDI-070820/113
agentejo					
cockpit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-06-2020	4.3	An issue was discovered in Agentejo Cockpit 0.10.2. Insufficient sanitization of the to parameter in the /auth/login route allows for injection of arbitrary JavaScript code into a web page's content, creating a Reflected XSS attack vector. **CVE ID : CVE-2020-14408**	N/A	A-AGE-COCK-070820/114
alpine_project					
alpine					
Information Exposure	19-06-2020	5	Alpine before 2.23 silently proceeds to use an insecure connection after a /tls is sent in certain circumstances	N/A	A-ALP-ALPI-070820/115

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			involving PREAUTH, which is a less secure behavior than the alternative of closing the connection and letting the user decide what they would like to do. **CVE ID : CVE-2020-14929**		
Apache					
tomcat					
Uncontrolled Resource Consumption	26-06-2020	5	A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive. **CVE ID : CVE-2020-11996**	https://lists.apache.org/thread.html/r5541ef6b6b68b49f76fc4c45695940116da2bcbe0312ef204a00a2e0%40%3Cannounce.tomcat.apache.org%3E, https://security.netapp.com/advisory/ntap-20200709-0002/	A-APA-TOMC-070820/116
Incorrect Default Permissions	29-06-2020	7.2	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-	https://bugzilla.suse.com/show_bug.cgi?id=1172405	A-APA-TOMC-070820/117

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1. **CVE ID : CVE-2020-8022**		
skywalking					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-06-2020	5	**Resolved** When use H2/MySQL/TiDB as Apache SkyWalking storage, the metadata query through GraphQL protocol, there is a SQL injection vulnerability, which allows to access unpexcted data. Apache SkyWalking 6.0.0 to 6.6.0, 7.0.0 H2/MySQL/TiDB storage implementations don't use the appropriate way to set SQL parameters. **CVE ID : CVE-2020-9483**	N/A	A-APA-SKYW-070820/118
activemq_artemis					
Insufficiently Protected Credentials	26-06-2020	2.1	A flaw was found in ActiveMQ Artemis management API from version 2.7.0 up until 2.12.0, where a user inadvertently stores passwords in plaintext in the Artemis	https://bugzilla.redhat.com/show_bug.cgi?id=1827200	A-APA-ACTI-070820/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			shadow file (etc/artemis-users.properties file) when executing the `resetUsers` operation. A local attacker can use this flaw to read the contents of the Artemis shadow file. **CVE ID : CVE-2020-10727**		
traffic_server					
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-06-2020	5	Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.10, and 8.0.0 to 8.0.7 is vulnerable to certain types of HTTP/2 HEADERS frames that can cause the server to allocate a large amount of memory and spin the thread. **CVE ID : CVE-2020-9494**	https://lists.apache.org/thread.html/rf7f86917f42fdaf904d99560cba0c016e03baea6244c47efeb60ecbe%40%3Cdev.trafficserver.apache.org%3E	A-APA-TRAF-070820/120
spark					
Improper Authentication	23-06-2020	9.3	In Apache Spark 2.4.5 and earlier, a standalone resource manager's master may be configured to require authentication (spark.authenticate) via a shared secret. When enabled, however, a specially-crafted RPC to the master can succeed in starting an application's resources on the Spark cluster, even without the shared key. This can be leveraged to execute shell commands on the host machine. This does not affect	https://spark.apache.org/security.html#CVE-2020-9480	A-APA-SPAR-070820/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Spark clusters using other resource managers (YARN, Mesos, etc). **CVE ID : CVE-2020-9480**		
archiva					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	19-06-2020	5	Apache Archiva login service before 2.2.5 is vulnerable to LDAP injection. A attacker is able to retrieve user attribute data from the connected LDAP server by providing special values to the login form. With certain characters it is possible to modify the LDAP filter used to query the LDAP users. By measuring the response time for the login request, arbitrary attribute data can be retrieved from LDAP user objects. **CVE ID : CVE-2020-9495**	N/A	A-APA-ARCH-070820/122
shiro					
Improper Authentication	22-06-2020	7.5	Apache Shiro before 1.5.3, when using Apache Shiro with Spring dynamic controllers, a specially crafted request may cause an authentication bypass. **CVE ID : CVE-2020-11989**	N/A	A-APA-SHIR-070820/123
apnswift_project					
apnswift					
Heap-based Buffer Overflow	22-06-2020	7.5	In APNSwift 1.0.0, calling APNSwiftSigner.sign(digest:) is likely to result in a heap buffer overflow. This has been fixed in 1.0.1.	https://github.com/kylebrowning/APNSwift/security/advisories/GHS	A-APN-APNS-070820/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4068	A-qh2w-vjxg-mjcg	
argent					
recoverymanager					
Missing Encryption of Sensitive Data	25-06-2020	5	In Argent RecoveryManager before 0xdc350d09f71c48c5D22fBE2741e4d6A03970E192, the executeRecovery function does not require any signatures in the zero-guardian case, which allows attackers to cause a denial of service (locking) or a takeover. **CVE ID : CVE-2020-15302**	N/A	A-ARG-RECO-070820/125
ARM					
mbed-coap					
Improper Release of Memory Before Removing Last Reference	18-06-2020	5	Memory leaks were discovered in the CoAP library in Arm Mbed OS 5.15.3 when using the Arm mbed-coap library 5.1.5. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses the CoAP option number field of all options present in the input packet. Each option number is calculated as a sum of the previous option number and a delta of the current option. The delta and the previous option number are expressed as unsigned 16-bit integers. Due to lack of overflow detection, it is	https://github.com/ARMmbed/mbed-coap/pull/116	A-ARM-MBED-070820/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possible to craft a packet that wraps the option number around and results in the same option number being processed again in a single packet. Certain options allocate memory by calling a memory allocation function. In the cases of COAP_OPTION_URI_QUERY, COAP_OPTION_URI_PATH, COAP_OPTION_LOCATION_QUERY, and COAP_OPTION_ETAG, there is no check on whether memory has already been allocated, which in conjunction with the option number integer overflow may lead to multiple assignments of allocated memory to a single pointer. This has been demonstrated to lead to memory leak by buffer orphaning. As a result, the memory is never freed. **CVE ID : CVE-2020-12887**		
arswp					
windows_cleanup_assistant					
Improper Input Validation	30-06-2020	6.1	In Windows cleaning assistant 3.2, the driver file (AtpKrnl.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x223CCA. **CVE ID : CVE-2020-14956**	N/A	A-ARS-WIND-070820/127

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	30-06-2020	6.1	In Windows cleaning assistant 3.2, the driver file (AtpKrnl.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x223CCD. **CVE ID : CVE-2020-14957**	N/A	A-ARS-WIND-070820/128
articatech					
artica_proxy					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-06-2020	5	Artica Proxy before 4.30.000000 Community Edition allows Directory Traversal via the fw.progrss.details.php popup parameter. **CVE ID : CVE-2020-13158**	N/A	A-ART-ARTI-070820/129
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-06-2020	10	Artica Proxy before 4.30.000000 Community Edition allows OS command injection via the Netbios name, Server domain name, dhclient_mac, Hostname, or Alias field. NOTE: this may overlap CVE-2020-10818. **CVE ID : CVE-2020-13159**	N/A	A-ART-ARTI-070820/130
Atlassian					
jira					
Information Exposure Through Discrepancy	23-06-2020	5	Versions before 8.9.1, Various resources in Jira responded with a 404 instead of redirecting unauthenticated users to the login page, in some situations this may have	N/A	A-ATL-JIRA-070820/131

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowed unauthorised attackers to determine if certain resources exist or not through an Information Disclosure vulnerability. **CVE ID : CVE-2020-4028**		
jira_software_data_center					
Information Exposure Through Discrepancy	23-06-2020	5	Versions before 8.9.1, Various resources in Jira responded with a 404 instead of redirecting unauthenticated users to the login page, in some situations this may have allowed unauthorised attackers to determine if certain resources exist or not through an Information Disclosure vulnerability. **CVE ID : CVE-2020-4028**	N/A	A-ATL-JIRA-070820/132
auth0					
express-jwt					
Improper Authorization	30-06-2020	4.3	In express-jwt (NPM package) up and including version 5.3.3, the algorithms entry to be specified in the configuration is not being enforced. When algorithms is not specified in the configuration, with the combination of jwks-rsa, it may lead to authorization bypass. You are affected by this vulnerability if all of the following conditions apply: - You are using express-jwt - You do not have **algorithms** configured in your express-jwt	https://github.com/auth0/express-jwt/security/advisories/GHSA-6g6m-m6h5-w9gf	A-AUT-EXPR-070820/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration. - You are using libraries such as jwks-rsa as the **secret**. You can fix this by specifying **algorithms** in the express-jwt configuration. See linked GHSA for example. This is also fixed in version 6.0.0. **CVE ID : CVE-2020-15084**		
Avast					
avg_antivirus					
Improper Privilege Management	29-06-2020	2.1	An elevation of privilege vulnerability exists in Avast Free Antivirus and AVG AntiVirus Free before 20.4 due to improperly handling hard links. The vulnerability allows local users to take control of arbitrary files. **CVE ID : CVE-2020-13657**	https://forum.avast.com/index.php?topic=232423.0, https://forum.avast.com/index.php?topic=234638.0	A-AVA-AVG_-070820/134
free_antivirus					
Improper Privilege Management	29-06-2020	2.1	An elevation of privilege vulnerability exists in Avast Free Antivirus and AVG AntiVirus Free before 20.4 due to improperly handling hard links. The vulnerability allows local users to take control of arbitrary files. **CVE ID : CVE-2020-13657**	https://forum.avast.com/index.php?topic=232423.0, https://forum.avast.com/index.php?topic=234638.0	A-AVA-FREE-070820/135
bdtask					
multi-scheduler					
Cross-Site Request Forgery	22-06-2020	4.3	The Multi-Scheduler plugin 1.0.0 for WordPress has a Cross-Site Request Forgery	N/A	A-BDT-MULT-070820/136

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			(CSRF) vulnerability in the forms it presents, allowing the possibility of deleting records (users) when an ID is known. **CVE ID : CVE-2020-13426**		
Beckhoff					
twincat_driver					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	https://cert.vde.com/en-us/advisories/vde-2020-019	A-BEC-TWIN-070820/137
twincat					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	https://cert.vde.com/en-us/advisories/vde-2020-019	A-BEC-TWIN-070820/138
Bitdefender					
total_security_2020					
Improper Input Validation	22-06-2020	6.8	Improper Input Validation vulnerability in the Safepay browser component of Bitdefender Total Security 2020 allows an external, specially crafted web page to run remote commands inside the Safepay Utility	N/A	A-BIT-TOTA-070820/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process. This issue affects Bitdefender Total Security 2020 versions prior to 24.0.20.116. **CVE ID : CVE-2020-8102**		
bitrix24					
bitrix24					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	4.3	The Web Application Firewall in Bitrix24 through 20.0.0 allows XSS via the items[ITEMS][ID] parameter to the components/bitrix/mobileapp.list/ajax.php/ URI. **CVE ID : CVE-2020-13483**	N/A	A-BIT-BITR-070820/140
Server-Side Request Forgery (SSRF)	24-06-2020	7.5	Bitrix24 through 20.0.975 allows SSRF via an intranet IP address in the services/main/ajax.php?action=attachUrlPreview url parameter, if the destination URL hosts an HTML document containing '<meta name="og:image" content="' followed by an intranet URL. **CVE ID : CVE-2020-13484**	N/A	A-BIT-BITR-070820/141
bludit					
bludit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	Bludit 3.12.0 allows stored XSS via JavaScript code in an SVG document to bl-kernel/ajax/logo-upload.php. **CVE ID : CVE-2020-15006**	N/A	A-BLU-BLUD-070820/142
Improper Limitation of	24-06-2020	4	Bludit 3.12.0 allows admins to use a /plugin-backup-	N/A	A-BLU-BLUD-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			download?file=../ directory traversal approach for arbitrary file download via backup/plugin.php. **CVE ID : CVE-2020-15026**		070820/143
boolebox					
boolebox					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	8.5	BooleBox Secure File Sharing Utility (potentially all versions) allows CSV injection via a crafted user name that is mishandled during export from the activity logs in the Audit Area. **CVE ID : CVE-2020-13247**	N/A	A-BOO-BOOL-070820/144
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	BooleBox Secure File Sharing Utility (potentially all versions) allows stored XSS via a crafted avatar field within My Account JSON data to Account.aspx. **CVE ID : CVE-2020-13248**	N/A	A-BOO-BOOL-070820/145
bt_ctroms_terminal_project					
bt_ctroms_terminal					
Improper Authentication	19-06-2020	4.3	An issue was discovered in BT CTROMS Terminal OS Port Portal CT-464. Account takeover can occur because the password-reset feature discloses the verification token. Upon a getverificationcode.jsp request, this token is transmitted not only to the registered phone number of the user account, but is also	N/A	A-BT_-BT_C-070820/146

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			transmitted to the unauthenticated HTTP client. **CVE ID : CVE-2020-14930**		
Cacti					
cacti					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-06-2020	6.5	A SQL injection issue in color.php in Cacti 1.2.12 allows an admin to inject SQL via the filter parameter. This can lead to remote command execution because the product accepts stacked queries. **CVE ID : CVE-2020-14295**	N/A	A-CAC-CACT-070820/147
Cakefoundation					
cakephp					
Cross-Site Request Forgery (CSRF)	30-06-2020	4.3	CakePHP before 4.0.6 mishandles CSRF token generation. This might be remotely exploitable in conjunction with XSS. **CVE ID : CVE-2020-15400**	N/A	A-CAK-CAKE-070820/148
casperjs					
casperjs					
Improper Input Validation	19-06-2020	7.5	In all versions of package casperjs, the mergeObjects utility function is susceptible to Prototype Pollution. **CVE ID : CVE-2020-7679**	N/A	A-CAS-CASP-070820/149
chocolate-doom					
chocolate_doom					
Buffer Copy without Checking Size of Input	22-06-2020	7.5	The server in Chocolate Doom 3.0.0 and Crispy Doom 5.8.0 doesn't validate the user-controlled num_players	N/A	A-CHO-CHOC-070820/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			value, leading to a buffer overflow. A malicious user can overwrite the server's stack. **CVE ID : CVE-2020-14983**		
crispy_doom					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	The server in Chocolate Doom 3.0.0 and Crispy Doom 5.8.0 doesn't validate the user-controlled num_players value, leading to a buffer overflow. A malicious user can overwrite the server's stack. **CVE ID : CVE-2020-14983**	N/A	A-CHO-CRIS-070820/151
Cisco					
clam_antivirus					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-06-2020	3.3	A vulnerability in the endpoint software of Cisco AMP for Endpoints and Clam AntiVirus could allow an authenticated, local attacker to cause the running software to delete arbitrary files on the system. The vulnerability is due to a race condition that could occur when scanning malicious files. An attacker with local shell access could exploit this vulnerability by executing a script that could trigger the race condition. A successful exploit could allow the attacker to delete arbitrary files on the system that the attacker would not normally have privileges to delete, producing system	N/A	A-CIS-CLAM-070820/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			instability or causing the endpoint software to stop working. **CVE ID : CVE-2020-3350**		
enterprise_network_function_virtualization_infrastructure					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-06-2020	7.2	A vulnerability in the CLI of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an authenticated, local attacker to gain root shell access to the underlying operating system and overwrite or read arbitrary files. The attacker would need valid administrative credentials. This vulnerability is due to improper input validation of CLI command arguments. An attacker could exploit this vulnerability by using path traversal techniques when executing a vulnerable command. A successful exploit could allow the attacker to gain root shell access to the underlying operating system and overwrite or read arbitrary files on an affected device. **CVE ID : CVE-2020-3236**	N/A	A-CIS-ENTE-070820/153
ucs_director					
Improper Limitation of a Pathname to a Restricted Directory ('Path	18-06-2020	8.5	A vulnerability in the orchestration tasks of Cisco UCS Director could allow an authenticated, remote attacker to perform a path traversal attack on an affected device. The	N/A	A-CIS-UCS_-070820/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			vulnerability is due to insufficient validation of user-supplied input on the web-based management interface. An attacker could exploit this vulnerability by creating a task with specific configuration parameters. A successful exploit could allow the attacker to overwrite arbitrary files in the file system of an affected device. **CVE ID : CVE-2020-3241**		
Information Exposure	18-06-2020	4	A vulnerability in the REST API of Cisco UCS Director could allow an authenticated, remote attacker with administrative privileges to obtain confidential information from an affected device. The vulnerability exists because confidential information is returned as part of an API response. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to obtain the API key of another user, which would allow the attacker to impersonate the account of that user on the affected device. To exploit this vulnerability, the attacker must have administrative privileges on the device. **CVE ID : CVE-2020-3242**	N/A	A-CIS-UCS_-070820/155

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
roomos					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	A vulnerability in the software upgrade process of Cisco TelePresence Collaboration Endpoint Software and Cisco RoomOS Software could allow an authenticated, remote attacker to modify the filesystem to cause a denial of service (DoS) or gain privileged access to the root filesystem. The vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending requests with malformed parameters to the system using the console, Secure Shell (SSH), or web API. A successful exploit could allow the attacker to modify the device configuration or cause a DoS. **CVE ID : CVE-2020-3336**	N/A	A-CIS-ROOM-070820/156
network_services_orchestrator					
Information Exposure	18-06-2020	1.9	A vulnerability in the CLI of Cisco Network Services Orchestrator (NSO) could allow an authenticated, local attacker to access confidential information on an affected device. The vulnerability is due to a timing issue in the processing of CLI commands. An attacker could exploit this vulnerability by	N/A	A-CIS-NETW-070820/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executing a specific sequence of commands on the CLI. A successful exploit could allow the attacker to read configuration information that would normally be accessible to administrators only. **CVE ID : CVE-2020-3362**		
data_center_network_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2020	3.5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need administrative credentials on the affected device. **CVE ID : CVE-2020-3354**	N/A	A-CIS-DATA-070820/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2020	3.5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker would need administrative credentials on the affected device. **CVE ID : CVE-2020-3355**	N/A	A-CIS-DATA-070820/159
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2020	4.3	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient input validation by the web-based	N/A	A-CIS-DATA-070820/160

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface. An attacker could exploit this vulnerability by interacting with the interface in a way that injects malicious content in a log file. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3356**		
umbrella					
URL Redirection to Untrusted Site ('Open Redirect')	18-06-2020	5.8	A vulnerability in the web server of Cisco Umbrella could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. The vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request that could cause the web application to redirect the request to a specified malicious URL. A successful exploit could allow the attacker to redirect a user to a malicious website. **CVE ID : CVE-2020-3337**	N/A	A-CIS-UMBR-070820/161
webex_meetings_server					
Improper Authenticati	18-06-2020	7.5	A vulnerability in Cisco Webex Meetings and Cisco	N/A	A-CIS-WEBE-070820/162

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			Webex Meetings Server could allow an unauthenticated, remote attacker to gain unauthorized access to a vulnerable Webex site. The vulnerability is due to improper handling of authentication tokens by a vulnerable Webex site. An attacker could exploit this vulnerability by sending crafted requests to a vulnerable Cisco Webex Meetings or Cisco Webex Meetings Server site. If successful, the attacker could gain the privileges of another user within the affected Webex site. **CVE ID : CVE-2020-3361**		
advanced_malware_protection_for_endpoints					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	18-06-2020	3.3	A vulnerability in the endpoint software of Cisco AMP for Endpoints and Clam AntiVirus could allow an authenticated, local attacker to cause the running software to delete arbitrary files on the system. The vulnerability is due to a race condition that could occur when scanning malicious files. An attacker with local shell access could exploit this vulnerability by executing a script that could trigger the race condition. A successful exploit could allow the attacker to delete	N/A	A-CIS-ADVA-070820/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary files on the system that the attacker would not normally have privileges to delete, producing system instability or causing the endpoint software to stop working. **CVE ID : CVE-2020-3350**		
webex_meetings					
Improper Certificate Validation	18-06-2020	9.3	A vulnerability in the software update feature of Cisco Webex Meetings Desktop App for Mac could allow an unauthenticated, remote attacker to execute arbitrary code on an affected system. The vulnerability is due to improper validation of cryptographic protections on files that are downloaded by the application as part of a software update. An attacker could exploit this vulnerability by persuading a user to go to a website that returns files to the client that are similar to files that are returned from a valid Webex website. The client may fail to properly validate the cryptographic protections of the provided files before executing them as part of an update. A successful exploit could allow the attacker to execute arbitrary code on the affected system with the privileges of the user. **CVE ID : CVE-2020-3342**	N/A	A-CIS-WEBE-070820/164

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-06-2020	2.1	A vulnerability in Cisco Webex Meetings Desktop App for Windows could allow an authenticated, local attacker to gain access to sensitive information on an affected system. The vulnerability is due to unsafe usage of shared memory that is used by the affected software. An attacker with permissions to view system memory could exploit this vulnerability by running an application on the local system that is designed to read shared memory. A successful exploit could allow the attacker to retrieve sensitive information from the shared memory, including usernames, meeting information, or authentication tokens that could aid the attacker in future attacks. **CVE ID : CVE-2020-3347**	N/A	A-CIS-WEBE-070820/165
Improper Input Validation	18-06-2020	7.6	A vulnerability in Cisco Webex Meetings Desktop App could allow an unauthenticated, remote attacker to execute programs on an affected end-user system. The vulnerability is due to improper validation of input that is supplied to application URLs. The attacker could exploit this vulnerability by persuading a user to follow a malicious	N/A	A-CIS-WEBE-070820/166

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			URL. A successful exploit could allow the attacker to cause the application to execute other programs that are already present on the end-user system. If malicious files are planted on the system or on an accessible network file path, the attacker could execute arbitrary code on the affected system. **CVE ID : CVE-2020-3263**		
Improper Authenticati on	18-06-2020	7.5	A vulnerability in Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to gain unauthorized access to a vulnerable Webex site. The vulnerability is due to improper handling of authentication tokens by a vulnerable Webex site. An attacker could exploit this vulnerability by sending crafted requests to a vulnerable Cisco Webex Meetings or Cisco Webex Meetings Server site. If successful, the attacker could gain the privileges of another user within the affected Webex site. **CVE ID : CVE-2020-3361**	N/A	A-CIS-WEBE-070820/167
telepresence_collaboration_endpoint					
Improper Neutralizatio n of Special	18-06-2020	9	A vulnerability in the software upgrade process of Cisco TelePresence	N/A	A-CIS-TELE-070820/168

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Collaboration Endpoint Software and Cisco RoomOS Software could allow an authenticated, remote attacker to modify the filesystem to cause a denial of service (DoS) or gain privileged access to the root filesystem. The vulnerability is due to insufficient input validation. An attacker with administrative privileges could exploit this vulnerability by sending requests with malformed parameters to the system using the console, Secure Shell (SSH), or web API. A successful exploit could allow the attacker to modify the device configuration or cause a DoS. **CVE ID : CVE-2020-3336**		
smart_software_manager_on-prem					
Missing Authorization	18-06-2020	5	A vulnerability in the web application of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to create arbitrary user accounts. The vulnerability is due to the lack of authorization controls in the web application. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the	N/A	A-CIS-SMAR-070820/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to add user accounts to the configuration of an affected device. These accounts would not be administrator or operator accounts. **CVE ID : CVE-2020-3245**		
Cisofy					
lynis					
Time-of-check Time-of-use (TOCTOU) Race Condition	18-06-2020	3.7	CISOfy Lynis before 3.0.0 has Incorrect Access Control because of a TOCTOU race condition. The routine to check the log and report file permissions was not working as intended and could be bypassed locally. Because of the race, an unprivileged attacker can set up a log and report file, and control that up to the point where the specific routine is doing its check. After that, the file can be removed, recreated, and used for additional attacks. **CVE ID : CVE-2020-13882**	https://cisofy.com/security/cve/cve-2020-13882/	A-CIS-LYNI-070820/170
Cmsmadesimple					
cms_made_simple					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2020	3.5	CMS Made Simple 2.2.14 allows XSS via a Search Term to the admin/moduleinterface.php?mact=ModuleManager page. **CVE ID : CVE-2020-14926**	N/A	A-CMS-CMS_-070820/171
compression_and_archive_extensions_project					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
compression_and_archive_extensions_zip_project					
Improper Input Validation	23-06-2020	5	In all versions of the package github.com/unknwon/cae/zip, the ExtractTo function doesn't securely escape file paths in zip archives which include leading or non-leading "..". This allows an attacker to add or replace files system-wide. **CVE ID : CVE-2020-7664**	N/A	A-COM-COMP-070820/172
compression_and_archive_extensions_tz_project					
Improper Input Validation	23-06-2020	5	In all versions of the package github.com/unknwon/cae/tz, the ExtractTo function doesn't securely escape file paths in zip archives which include leading or non-leading "..". This allows an attacker to add or replace files system-wide. **CVE ID : CVE-2020-7668**	N/A	A-COM-COMP-070820/173
Concrete5					
concrete5					
N/A	22-06-2020	5	Concrete5 before 8.5.3 does not constrain the sort direction to a valid asc or desc value. **CVE ID : CVE-2020-14961**	N/A	A-CON-CONC-070820/174
convos					
convos					
Use of Insufficiently Random Values	18-06-2020	5	Convos before 4.20 does not properly generate a random secret in Core/Settings.pm and Util.pm. This leads to a predictable CONVOS_LOCAL_SECRET	N/A	A-CON-CONV-070820/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			value, affecting password resets and invitations. **CVE ID : CVE-2020-14423**		
coturn_project					
coturn					
Improper Initialization	29-06-2020	5	In coturn before version 4.5.1.3, there is an issue whereby STUN/TURN response buffer is not initialized properly. There is a leak of information between different client connections. One client (an attacker) could use their connection to intelligently query coturn to get interesting bytes in the padding bytes from the connection of another client. This has been fixed in 4.5.1.3. **CVE ID : CVE-2020-4067**	https://github.com/coturn/coturn/security/advisories/GHSA-c8r8-8vp5-6gcm	A-COT-COTU-070820/176
cyberark					
conjur_oss_helm_chart					
Improper Access Control	22-06-2020	7.7	In Conjur OSS Helm Chart before 2.0.0, a recently identified critical vulnerability resulted in the installation of the Conjur Postgres database with an open port. This allows an attacker to gain full read & write access to the Conjur Postgres database, including escalating the attacker's privileges to assume full control. A malicious actor who knows the IP address and port number of the	https://github.com/cyberark/conjur-oss-helm-chart/security/advisories/GHSA-mg2m-623j-wpxw	A-CYB-CONJ-070820/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Postgres database and has access into the Kubernetes cluster where Conjur runs can gain full read & write access to the Postgres database. This enables the attacker to write a policy that allows full access to retrieve any secret. This Helm chart is a method to install Conjur OSS into a Kubernetes environment. Hence, the systems impacted are only Conjur OSS systems that were deployed using this chart. Other deployments including Docker and the CyberArk Dynamic Access Provider (DAP) are not affected. To remediate this vulnerability, clone the latest Helm Chart and follow the upgrade instructions. If you are not able to fully remediate this vulnerability immediately, you can mitigate some of the risk by making sure Conjur OSS is deployed on an isolated Kubernetes cluster or namespace. The term "isolated" refers to: - No other workloads besides Conjur OSS and its backend database are running in that Kubernetes cluster/namespace. - Kubernetes and helm access to the cluster/namespace is limited to security administrators via Role-		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Based Access Control (RBAC). **CVE ID : CVE-2020-4062**		
Cybozu					
garoon					
Improper Privilege Management	30-06-2020	5.5	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to view and/or alter Single sign-on settings via unspecified vectors. **CVE ID : CVE-2020-5580**	N/A	A-CYB-GARO-070820/178
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-06-2020	4	Path traversal vulnerability in Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to obtain unintended information via unspecified vectors. **CVE ID : CVE-2020-5581**	N/A	A-CYB-GARO-070820/179
Incorrect Authorizatio n	30-06-2020	4	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to alter the data for the file attached to Report via unspecified vectors. **CVE ID : CVE-2020-5582**	N/A	A-CYB-GARO-070820/180
Information Exposure	30-06-2020	4	Cybozu Garoon 4.0.0 to 5.0.1 allows remote authenticated attackers to bypass access restriction to obtain unauthorized Multi-Report's data via unspecified vectors. **CVE ID : CVE-2020-5583**	N/A	A-CYB-GARO-070820/181
Information Exposure	30-06-2020	5	Cybozu Garoon 4.0.0 to 5.0.1 allow remote attackers to	N/A	A-CYB-GARO-070820/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain unintended information via unspecified vectors. **CVE ID : CVE-2020-5584**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-06-2020	3.5	Cross-site scripting vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5585**	N/A	A-CYB-GARO-070820/183
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-06-2020	3.5	Cross-site scripting vulnerability in Cybozu Garoon 4.10.3 to 5.0.1 allows attacker with administrator rights to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5586**	N/A	A-CYB-GARO-070820/184
Information Exposure	30-06-2020	4	Cybozu Garoon 4.0.0 to 5.0.1 allow remote authenticated attackers to obtain unintended information via unspecified vectors. **CVE ID : CVE-2020-5587**	N/A	A-CYB-GARO-070820/185
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-06-2020	4	Path traversal vulnerability in Cybozu Garoon 5.0.0 to 5.0.1 allows attacker with administrator rights to obtain unintended information via unspecified vectors. **CVE ID : CVE-2020-5588**	N/A	A-CYB-GARO-070820/186
Dell					
emc_unisphere_for_powermax					
Missing	23-06-2020	5.5	Dell EMC Unisphere for	https://ww	A-DEL-EMC_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authorization			PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an authorization bypass vulnerability. An authenticated malicious user may potentially execute commands to alter or stop database statistics. **CVE ID : CVE-2020-5345**	w.dell.com/support/security/en-us/details/544585/DSA-2020-065-Dell-EMC-Unisphere-for-PowerMax-Dell-EMC-Unisphere-for-PowerMax-Virtual-Appliance	070820/187
Improper Certificate Validation	23-06-2020	6.8	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an improper certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim's data in transit. **CVE ID : CVE-2020-5367**	https://www.dell.com/support/security/en-us/details/544585/DSA-2020-065-Dell-EMC-Unisphere-for-PowerMax-Dell-EMC-Unisphere-for-PowerMax-Virtual-Appliance	A-DEL-EMC_-070820/188
emc_unisphere_for_powermax_virtual_appliance					
Missing Authorization	23-06-2020	5.5	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere	https://www.dell.com/support/sec	A-DEL-EMC_-070820/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an authorization bypass vulnerability. An authenticated malicious user may potentially execute commands to alter or stop database statistics. **CVE ID : CVE-2020-5345**	urity/en-us/details/544585/DSA-2020-065-Dell-EMC-Unisphere-for-PowerMax-Dell-EMC-Unisphere-for-PowerMax-Virtual-Appliance	
Improper Certificate Validation	23-06-2020	6.8	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an improper certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim's data in transit. **CVE ID : CVE-2020-5367**	https://www.dell.com/support/security/en-us/details/544585/DSA-2020-065-Dell-EMC-Unisphere-for-PowerMax-Dell-EMC-Unisphere-for-PowerMax-Virtual-Appliance	A-DEL-EMC_-070820/190
deltaww					
dopsoft					
Out-of-bounds Write	30-06-2020	6.8	Delta Industrial Automation DOPSoft, Version 4.00.08.15 and prior. Opening a specially crafted project file	N/A	A-DEL-DOPS-070820/191

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may overflow the heap, which may allow remote code execution, disclosure/modification of information, or cause the application to crash. **CVE ID : CVE-2020-14482**		
django-basic-auth-ip-whitelist_project					
django-basic-auth-ip-whitelist					
Information Exposure Through Timing Discrepancy	24-06-2020	2.1	In django-basic-auth-ip-whitelist before 0.3.4, a potential timing attack exists on websites where the basic authentication is used or configured, i.e. BASIC_AUTH_LOGIN and BASIC_AUTH_PASSWORD is set. Currently the string comparison between configured credentials and the ones provided by users is performed through a character-by-character string comparison. This enables a possibility that attacker may time the time it takes the server to validate different usernames and password, and use this knowledge to work out the valid credentials. This attack is understood not to be realistic over the Internet. However, it may be achieved from within local networks where the website is hosted, e.g. from inside a data centre where a website's server is located. Sites protected by IP address whitelisting only are	https://github.com/tm-kn/django-basic-auth-ip-whitelist/security/advisories/GHSA-m38j-pmg3-v5x5	A-DJA-DJAN-070820/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unaffected by this vulnerability. This vulnerability has been fixed on version 0.3.4 of django-basic-auth-ip-whitelist. Update to version 0.3.4 as soon as possible and change basic authentication username and password configured on a Django project using this package. A workaround without upgrading to version 0.3.4 is to stop using basic authentication and use the IP whitelisting component only. It can be achieved by not setting BASIC_AUTH_LOGIN and BASIC_AUTH_PASSWORD in Django project settings. **CVE ID : CVE-2020-4071**		
dmitry_project					
dmitry					
Out-of-bounds Write	19-06-2020	7.5	A stack-based buffer overflow in DMitry (Deepmagic Information Gathering Tool) 1.3a might allow remote WHOIS servers to execute arbitrary code via a long line in a response that is mishandled by nic_format_buff. **CVE ID : CVE-2020-14931**	N/A	A-DMI-DMIT-070820/193
Docker					
docker_desktop					
Improper Privilege	27-06-2020	4.6	com.docker.vmnetd in Docker Desktop 2.3.0.3 allows privilege escalation	N/A	A-DOC-DOCK-070820/194

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			because of a lack of client verification. **CVE ID : CVE-2020-15360**		
Dolibarr					
dolibarr					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-06-2020	6.5	A SQL injection vulnerability in accountancy/customer/card.php in Dolibarr 11.0.3 allows remote authenticated users to execute arbitrary SQL commands via the id parameter. **CVE ID : CVE-2020-14443**	https://github.com/Dolibarr/dolibarr/commit/40e16672e3aa4e9208ea7a4829f30507dcdfc4ba	A-DOL-DOLI-070820/195
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2020	4.3	A reflected cross-site scripting (XSS) vulnerability in Dolibarr 11.0.3 allows remote attackers to inject arbitrary web script or HTML into public/notice.php (related to transphrase and transkey). **CVE ID : CVE-2020-14475**	N/A	A-DOL-DOLI-070820/196
doom_vanille_project					
doom_vanille					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-06-2020	7.5	A buffer overflow in the M_LoadDefaults function in m_misc.c in id Tech 1 (aka Doom engine) allows arbitrary code execution via an unsafe usage of fscanf, because it does not limit the number of characters to be read in a format argument. **CVE ID : CVE-2020-15007**	N/A	A-DOO-DOOM-070820/197
Ec-cube					
ec-cube					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-06-2020	5.5	Directory traversal vulnerability in EC-CUBE 3.0.0 to 3.0.18 and 4.0.0 to 4.0.3 allows remote authenticated attackers to delete arbitrary files and/or directories on the server via unspecified vectors. **CVE ID : CVE-2020-5590**	N/A	A-EC--EC-C-070820/198
exacq					
exacq					
Improper Verification of Cryptographic Signature	26-06-2020	9	A vulnerability exists that could allow the execution of unauthorized code or operating system commands on systems running exacqVision Web Service versions 20.06.3.0 and prior and exacqVision Enterprise Manager versions 20.06.4.0 and prior. An attacker with administrative privileges could potentially download and run a malicious executable that could allow OS command injection on the system. **CVE ID : CVE-2020-9047**	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	A-EXA-EXAC-070820/199
exacqvision_enterprise_manager					
Improper Verification of Cryptographic Signature	26-06-2020	9	A vulnerability exists that could allow the execution of unauthorized code or operating system commands on systems running exacqVision Web Service versions 20.06.3.0 and prior and exacqVision Enterprise Manager versions 20.06.4.0 and prior. An attacker with	https://www.johnsoncontrols.com/cyber-solutions/security-advisories	A-EXA-EXAC-070820/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges could potentially download and run a malicious executable that could allow OS command injection on the system. **CVE ID : CVE-2020-9047**		
Expressionengine					
expressionengine					
Unrestricted Upload of File with Dangerous Type	24-06-2020	6.5	ExpressionEngine before 5.3.2 allows remote attackers to upload and execute arbitrary code in a .php%20 file via Compose Msg, Add attachment, and Save As Draft actions. A user with low privileges (member) is able to upload this. It is possible to bypass the MIME type check and file-extension check while uploading new files. Short aliases are not used for an attachment; instead, direct access is allowed to the uploaded files. It is possible to upload PHP only if one has member access, or registration/forum is enabled and one can create a member with the default group id of 5. To exploit this, one must to be able to send and compose messages (at least). **CVE ID : CVE-2020-13443**	N/A	A-EXP-EXPR-070820/201
fabulatech					
usb_for_remote_desktop					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	17-06-2020	4.6	ftusbbus2.sys in FabulaTech USB for Remote Desktop through 2020-02-19 allows privilege escalation via crafted IoCtl code related to a USB HID device. **CVE ID : CVE-2020-9332**	N/A	A-FAB-USB_-070820/202
factorfx					
open_computer_software_inventory_next_generation					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-06-2020	6.5	OCS Inventory NG 2.7 allows Remote Command Execution via shell metacharacters to require/commandLine/CommandLine.php because mib_file in plugins/main_sections/ms_config/ms_snmp_config.php is mishandled in get_mib_oid. **CVE ID : CVE-2020-14947**	https://github.com/OCSInventory-NG/OCSInventory-ocsreports/commit/da72e0fddaeceee44fbbd7241e07e5d53d1eee64	A-FAC-OPEN-070820/203
Fasterxml					
jackson-databind					
Deserialization of Untrusted Data	16-06-2020	6.8	FasterXML jackson-databind 2.x before 2.9.10.5 mishandles the interaction between serialization gadgets and typing, related to org.jsecurity.realm.jndi.JndiRealmFactory (aka org.jsecurity). **CVE ID : CVE-2020-14195**	https://security.netapp.com/advisory/ntap-20200702-0003/	A-FAS-JACK-070820/204
Ffmpeg					
ffmpeg					
Out-of-bounds Write	16-06-2020	6.8	FFmpeg through 4.3 has a heap-based buffer overflow in avio_get_str in libavformat/aviobuf.c	N/A	A-FFM-FFMP-070820/205

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because dnn_backend_native.c calls ff_dnn_load_model_native and a certain index check is omitted. **CVE ID : CVE-2020-14212**		
form_builder_for_magento_2_project					
form_builder_for_magento_2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-06-2020	3.5	Form Builder 2.1.0 for Magento has multiple XSS issues that can be exploited against Magento 2 admin accounts via the Current_url or email field, or the User-Agent HTTP header. **CVE ID : CVE-2020-13423**	N/A	A-FOR-FORM-070820/206
Fortinet					
fortideceptor					
Insufficient Session Expiration	22-06-2020	6.8	An insufficient session expiration vulnerability in FortiDeceptor 3.0.0 and below allows an attacker to reuse the unexpired admin user session IDs to gain admin privileges, should the attacker be able to obtain that session ID via other, hypothetical attacks. **CVE ID : CVE-2020-6644**	https://fortiguard.com/advisory/FG-IR-20-006	A-FOR-FORT-070820/207
fortimanager					
Use of Hard-coded Credentials	16-06-2020	5	Use of a hard-coded cryptographic key to encrypt password data in CLI configuration in FortiManager 6.2.3 and below may allow an attacker with access to the CLI configuration or the CLI	N/A	A-FOR-FORT-070820/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			backup file to decrypt the sensitive data, via knowledge of the hard-coded key. **CVE ID : CVE-2020-9289**		
fortiwlc					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	3.5	An improper neutralization of input vulnerability in FortiWLC 8.5.1 allows a remote authenticated attacker to perform a stored cross site scripting attack (XSS) via the ESS profile or the Radius Profile. **CVE ID : CVE-2020-9288**	https://fortiguard.com/advisory/FG-IR-20-016	A-FOR-FORT-070820/209
freedroid					
freedroidrpg					
Out-of-bounds Write	23-06-2020	7.5	An issue was discovered in map.c in FreedroidRPG 1.0rc2. It assumes lengths of data sets read from saved game files. It copies data from a file into a fixed-size heap-allocated buffer without size verification, leading to a heap-based buffer overflow. **CVE ID : CVE-2020-14938**	N/A	A-FRE-FREE-070820/210
Improper Input Validation	23-06-2020	6.8	An issue was discovered in savestruct_internal.c in FreedroidRPG 1.0rc2. Saved game files are composed of Lua scripts that recover a game's state. A file can be modified to put any Lua code inside, leading to arbitrary code execution while loading.	N/A	A-FRE-FREE-070820/211

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14939		
freerdp					
freerdp					
Out-of-bounds Read	22-06-2020	5.5	In FreeRDP before version 2.1.2, an out of bound reads occurs resulting in accessing a memory location that is outside of the boundaries of the static array PRIMARY_DRAWING_ORDER_FIELD_BYTES. This is fixed in version 2.1.2. **CVE ID : CVE-2020-11095**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-563r-pvh7-4fw2	A-FRE-FREE-070820/212
Out-of-bounds Read	22-06-2020	6.4	In FreeRDP before version 2.1.2, there is a global OOB read in update_read_cache_bitmap_v3_order. As a workaround, one can disable bitmap cache with -bitmap-cache (default). This is fixed in version 2.1.2. **CVE ID : CVE-2020-11096**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-mjw7-3mq2-996x	A-FRE-FREE-070820/213
Out-of-bounds Read	22-06-2020	5.5	In FreeRDP before version 2.1.2, an out of bounds read occurs resulting in accessing a memory location that is outside of the boundaries of the static array PRIMARY_DRAWING_ORDER_FIELD_BYTES. This is fixed in version 2.1.2. **CVE ID : CVE-2020-11097**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-c8x2-c3c9-9r3f	A-FRE-FREE-070820/214
Out-of-bounds Read	22-06-2020	5.8	In FreeRDP before version 2.1.2, there is an out-of-bound read in glyph_cache_put. This affects all FreeRDP clients with	https://github.com/FreeRDP/FreeRDP/security/advisori	A-FRE-FREE-070820/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			`+glyph-cache` option enabled This is fixed in version 2.1.2. **CVE ID : CVE-2020-11098**	es/GHSA-jr57-f58x-hjmv	
Out-of-bounds Read	22-06-2020	6.4	In FreeRDP before version 2.1.2, there is an out of bounds read in license_read_new_or_upgrade_license_packet. A manipulated license packet can lead to out of bound reads to an internal buffer. This is fixed in version 2.1.2. **CVE ID : CVE-2020-11099**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-977w-866x-4v5h	A-FRE-FREE-070820/216
Out-of-bounds Read	22-06-2020	6.4	In FreeRDP before version 2.1.2, there is an out of bounds read in TrioParse. Logging might bypass string length checks due to an integer overflow. This is fixed in version 2.1.2. **CVE ID : CVE-2020-4030**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-fjr5-97f5-qq98	A-FRE-FREE-070820/217
Use After Free	22-06-2020	4.3	In FreeRDP before version 2.1.2, there is a use-after-free in gdi_SelectObject. All FreeRDP clients using compatibility mode with /relax-order-checks are affected. This is fixed in version 2.1.2. **CVE ID : CVE-2020-4031**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-gwcq-hpq2-m74g	A-FRE-FREE-070820/218
Incorrect Conversion between Numeric Types	22-06-2020	6.8	In FreeRDP before version 2.1.2, there is an integer casting vulnerability in update_recv_secondary_order. All clients with +glyph-cache /relax-order-checks are affected. This is fixed in	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-3898-	A-FRE-FREE-070820/219

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 2.1.2. **CVE ID : CVE-2020-4032**	mc89-x2vc	
Out-of-bounds Read	22-06-2020	6.4	In FreeRDP before version 2.1.2, there is an out of bounds read in RLEDECOMPRESS. All FreeRDP based clients with sessions with color depth < 32 are affected. This is fixed in version 2.1.2. **CVE ID : CVE-2020-4033**	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-7rhj-856w-82p8	A-FRE-FREE-070820/220
F-secure					
safe					
Improper Input Validation	23-06-2020	9.3	An issue was discovered in F-Secure SAFE 17.7 on macOS. The XPC services use the PID to identify the connecting client, which allows an attacker to perform a PID reuse attack and connect to a privileged XPC service, and execute privileged commands on the system. NOTE: the attacker needs to execute code on an already compromised machine. **CVE ID : CVE-2020-14977**	N/A	A-F-S-SAFE-070820/221
Missing Authorization	23-06-2020	9.3	An issue was discovered in F-Secure SAFE 17.7 on macOS. Due to incorrect client version verification, an attacker can connect to a privileged XPC service, and execute privileged commands on the system. NOTE: the attacker needs to execute code on an already	N/A	A-F-S-SAFE-070820/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compromised machine. **CVE ID : CVE-2020-14978**		
geti2p					
i2p					
Incorrect Default Permissions	16-06-2020	7.2	I2P before 0.9.46 allows local users to gain privileges via a Trojan horse I2PSvc.exe file because of weak permissions on a certain %PROGRAMFILES% subdirectory. **CVE ID : CVE-2020-13431**	N/A	A-GET-I2P-070820/223
Gitlab					
gitlab-vscode-extension					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-06-2020	6.8	Client side code execution in gitlab-vscode-extension v2.2.0 allows attacker to execute code on user system **CVE ID : CVE-2020-13279**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13279.json	A-GIT-GITL-070820/224
gitlab					
Insufficiently Protected Credentials	19-06-2020	4	Amazon EKS credentials disclosure in GitLab CE/EE 12.6 and later through 13.0.1 allows other administrators to view Amazon EKS credentials via HTML source code **CVE ID : CVE-2020-13261**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13261.json	A-GIT-GITL-070820/225
Improper Neutralization of Input During Web Page	19-06-2020	4.3	Client-Side code injection through Mermaid markup in GitLab CE/EE 12.9 and later through 13.0.1 allows a specially crafted Mermaid	https://gitlab.com/gitlab-org/cves/-/blob/mast	A-GIT-GITL-070820/226

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			payload to PUT requests on behalf of other users via clicking on a link **CVE ID : CVE-2020-13262**	er/2020/CVE-2020-13262.json	
Incorrect Authorization	19-06-2020	6.5	An authorization issue relating to project maintainer impersonation was identified in GitLab EE 9.5 and later through 13.0.1 that could allow unauthorized users to impersonate as a maintainer to perform limited actions. **CVE ID : CVE-2020-13263**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13263.json	A-GIT-GITL-070820/227
Information Exposure	19-06-2020	5	Kubernetes cluster token disclosure in GitLab CE/EE 10.3 and later through 13.0.1 allows other group maintainers to view Kubernetes cluster token **CVE ID : CVE-2020-13264**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13264.json	A-GIT-GITL-070820/228
Insufficient Verification of Data Authenticity	19-06-2020	5	User email verification bypass in GitLab CE/EE 12.5 and later through 13.0.1 allows user to bypass email verification **CVE ID : CVE-2020-13265**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13265.json	A-GIT-GITL-070820/229
Incorrect Authorization	19-06-2020	6.5	OAuth flow missing verification checks CE/EE 12.3 and later through 13.0.1 allows unverified user to use OAuth authorization code flow **CVE ID : CVE-2020-13272**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13272.json	A-GIT-GITL-070820/230
Uncontrolled	19-06-2020	7.8	A Denial of Service	https://gitl	A-GIT-GITL-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			vulnerability allowed exhausting the system resources in GitLab CE/EE 12.0 and later through 13.0.1 **CVE ID : CVE-2020-13273**	ab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13273.json	070820/231
Uncontrolled Resource Consumption	19-06-2020	5	A security issue allowed achieving Denial of Service attacks through memory exhaustion by uploading malicious artifacts in all previous GitLab versions through 13.0.1 **CVE ID : CVE-2020-13274**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13274.json	A-GIT-GITL-070820/232
Incorrect Authorization	19-06-2020	5.5	A user with an unverified email address could request an access to domain restricted groups in GitLab EE 12.2 and later through 13.0.1 **CVE ID : CVE-2020-13275**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13275.json	A-GIT-GITL-070820/233
Incorrect Authorization	19-06-2020	4	User is allowed to set an email as a notification email even without verifying the new email in all previous GitLab CE/EE versions through 13.0.1 **CVE ID : CVE-2020-13276**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13276.json	A-GIT-GITL-070820/234
Incorrect Authorization	19-06-2020	4	An authorization issue in the mirroring logic allowed read access to private repositories in GitLab CE/EE 10.6 and later through 13.0.5 **CVE ID : CVE-2020-13277**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13277.json	A-GIT-GITL-070820/235

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Gleamtech					
fileultimate					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	4.3	The FileExplorer component in GleamTech FileUltimate 6.1.5.0 allows XSS via an SVG document. **CVE ID : CVE-2020-15015**	N/A	A-GLE-FILE-070820/236
globalradar					
bsa_radar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	3.5	The Firstname and Lastname parameters in Global RADAR BSA Radar 1.6.7234.24750 and earlier are vulnerable to stored cross-site scripting (XSS) via Update User Profile. **CVE ID : CVE-2020-14943**	N/A	A-GLO-BSA_-070820/237
Incorrect Authorization	22-06-2020	7.5	Global RADAR BSA Radar 1.6.7234.24750 and earlier lacks valid authorization controls in multiple functions. This can allow for manipulation and takeover of user accounts if successfully exploited. The following vulnerable functions are exposed: ChangePassword, SaveUserProfile, and GetUser. **CVE ID : CVE-2020-14944**	N/A	A-GLO-BSA_-070820/238
Improper Privilege Management	22-06-2020	6.5	A privilege escalation vulnerability exists within Global RADAR BSA Radar 1.6.7234.24750 and earlier	N/A	A-GLO-BSA_-070820/239

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that allows an authenticated, low-privileged user to escalate their privileges to administrator rights (i.e., the BankAdmin role) via modified SaveUser data. **CVE ID : CVE-2020-14945**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-06-2020	4	downloadFile.ashx in the Administrator section of the Surveillance module in Global RADAR BSA Radar 1.6.7234.24750 and earlier allows users to download transaction files. When downloading the files, a user is able to view local files on the web server by manipulating the FileName and FilePath parameters in the URL, or while using a proxy. This vulnerability could be used to view local sensitive files or configuration files. **CVE ID : CVE-2020-14946**	N/A	A-GLO-BSA_-070820/240
Gns3					
ubridge					
Information Exposure	23-06-2020	4.9	GNS3 ubridge through 0.9.18 on macOS, as used in GNS3 server before 2.1.17, allows a local attacker to read arbitrary files because it handles configuration-file errors by printing the configuration file while executing in a setuid root context. **CVE ID : CVE-2020-14976**	N/A	A-GNS-UBRI-070820/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gns3					
Information Exposure	23-06-2020	4.9	GNS3 ubridge through 0.9.18 on macOS, as used in GNS3 server before 2.1.17, allows a local attacker to read arbitrary files because it handles configuration-file errors by printing the configuration file while executing in a setuid root context. **CVE ID : CVE-2020-14976**	N/A	A-GNS-GNS3-070820/242
GNU					
mailman					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	2.6	GNU Mailman before 2.1.33 allows arbitrary content injection via the Cgi/private.py private archive login page. **CVE ID : CVE-2020-15011**	N/A	A-GNU-MAIL-070820/243
gogs					
gogs					
Improper Preservation of Permissions	21-06-2020	4	In Gogs 0.11.91, MakeEmailPrimary in models/user_mail.go lacks a "not the owner of the email" check. **CVE ID : CVE-2020-14958**	N/A	A-GOG-GOGS-070820/244
Golang					
text					
Loop with Unreachable Exit Condition	17-06-2020	5	The x/text package before 0.3.3 for Go has a vulnerability in encoding/unicode that could	N/A	A-GOL-TEXT-070820/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			lead to the UTF-16 decoder entering an infinite loop, causing the program to crash or run out of memory. An attacker could provide a single byte to a UTF16 decoder instantiated with UseBOM or ExpectBOM to trigger an infinite loop if the String function on the Decoder is called, or the Decoder is passed to golang.org/x/text/transform .String. **CVE ID : CVE-2020-14040**		
Goldplugins					
easy_testimonials					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	3.5	Multiple XSS vulnerabilities in the Easy Testimonials plugin before 3.6 for WordPress allow remote attackers to inject arbitrary web script or HTML via the wp-admin/post.php Client Name, Position, Web Address, Other, Location Reviewed, Product Reviewed, Item Reviewed, or Rating parameter. **CVE ID : CVE-2020-14959**	N/A	A-GOL-EASY-070820/246
Google					
guest-oslogin					
Incorrect Default Permissions	22-06-2020	6.9	A vulnerability in Google Cloud Platform's guest-oslogin versions between 20190304 and 20200507 allows a user that is only granted the role "roles/compute.osLogin" to	https://github.com/GoogleCloudPlatform/guest-oslogin/pull	A-GOO-GUES-070820/247

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges to root. Using their membership to the "adm" group, users with this role are able to read the DHCP XID from the systemd journal. Using the DHCP XID, it is then possible to set the IP address and hostname of the instance to any value, which is then stored in /etc/hosts. An attacker can then point metadata.google.internal to an arbitrary IP address and impersonate the GCE metadata server which make it is possible to instruct the OS Login PAM module to grant administrative privileges. All images created after 2020-May-07 (20200507) are fixed, and if you cannot update, we recommend you edit /etc/group/security.conf and remove the "adm" user from the OS Login entry. **CVE ID : CVE-2020-8903**	/29	
Incorrect Default Permissions	22-06-2020	6.9	A vulnerability in Google Cloud Platform's guest-oslogin versions between 20190304 and 20200507 allows a user that is only granted the role "roles/compute.osLogin" to escalate privileges to root. Using their membership to the "docker" group, an attacker with this role is able to run docker and mount the host OS. Within docker, it is	https://github.com/GoogleCloudPlatform/guest-oslogin/pull/29	A-GOO-GUES-070820/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possible to modify the host OS filesystem and modify /etc/groups to gain administrative privileges. All images created after 2020-May-07 (20200507) are fixed, and if you cannot update, we recommend you edit /etc/group/security.conf and remove the "docker" user from the OS Login entry. **CVE ID : CVE-2020-8907**		
Incorrect Default Permissions	22-06-2020	6.9	A vulnerability in Google Cloud Platform's guest-oslogin versions between 20190304 and 20200507 allows a user that is only granted the role "roles/compute.osLogin" to escalate privileges to root. Using the membership to the "lxd" group, an attacker can attach host devices and filesystems. Within an lxc container, it is possible to attach the host OS filesystem and modify /etc/sudoers to then gain administrative privileges. All images created after 2020-May-07 (20200507) are fixed, and if you cannot update, we recommend you edit /etc/group/security.conf and remove the "lxd" user from the OS Login entry. **CVE ID : CVE-2020-8933**	https://github.com/GoogleCloudPlatform/guest-oslogin/pull/29	A-GOO-GUES-070820/249
gvectors					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wpdiscuz					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-06-2020	7.5	A SQL injection issue in the gVectors wpDiscuz plugin 5.3.5 and earlier for WordPress allows remote attackers to execute arbitrary SQL commands via the order parameter of a wpdLoadMoreComments request. (No 7.x versions are affected.) **CVE ID : CVE-2020-13640**	N/A	A-GVE-WPDI-070820/250
hcltech					
notes					
Information Exposure	26-06-2020	4.3	HCL Notes is vulnerable to an information leakage vulnerability through its support for the 'mailto' protocol. This vulnerability could result in files from the user's filesystem or connected network filesystems being leaked to a third party. All versions of HCL Notes 9, 10 and 11 are affected. **CVE ID : CVE-2020-4089**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0080343	A-HCL-NOTE-070820/251
heinekingmedia					
stashcat					
Cleartext Storage of Sensitive Information	17-06-2020	5	An issue was discovered in the stashcat app through 3.9.2 for macOS, Windows, Android, iOS, and possibly other platforms. It stores the client_key, the device_id, and the public key for end-to-end encryption in cleartext, enabling an attacker (by	N/A	A-HEI-STAS-070820/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			copying or having access to the local storage database file) to login to the system from any other computer, and get unlimited access to all data in the users's context. **CVE ID : CVE-2020-13637**		
helm					
helm					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-06-2020	8.5	In Helm greater than or equal to 3.0.0 and less than 3.2.4, a path traversal attack is possible when installing Helm plugins from a tar archive over HTTP. It is possible for a malicious plugin author to inject a relative path into a plugin archive, and copy a file outside of the intended directory. This has been fixed in 3.2.4. **CVE ID : CVE-2020-4053**	https://github.com/helm/helm/security/advisories/GHSA-qq3j-xp49-j73f	A-HEL-HELM-070820/253
Herac					
tuxguitar					
Improper Restriction of XML External Entity Reference ('XXE')	23-06-2020	5	An issue was discovered in io/gpx/GPXDocumentReader.java in TuxGuitar 1.5.4. It uses misconfigured XML parsers, leading to XXE while loading GP6 (.gpx) and GP7 (.gp) tablature files. **CVE ID : CVE-2020-14940**	N/A	A-HER-TUXG-070820/254
hmtalk					
daoffice					
Out-of-	30-06-2020	6.8	A vulnerability in the JPEG	https://ww	A-HMT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			image parsing module in DaView Indy, DaVa+, DaOffice softwares could allow an unauthenticated, remote attacker to cause an arbitrary code execution on an affected device.nThe vulnerability is due to a stack overflow read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device. **CVE ID : CVE-2020-7816**	w.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35483	DAOF-070820/255
dava\+					
Out-of-bounds Write	30-06-2020	6.8	A vulnerability in the JPEG image parsing module in DaView Indy, DaVa+, DaOffice softwares could allow an unauthenticated, remote attacker to cause an arbitrary code execution on an affected device.nThe vulnerability is due to a stack overflow read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device. **CVE ID : CVE-2020-7816**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35483	A-HMT-DAVA-070820/256
daview_indy					
Out-of-bounds Write	30-06-2020	6.8	A vulnerability in the JPEG image parsing module in DaView Indy, DaVa+, DaOffice softwares could allow an unauthenticated, remote attacker to cause an arbitrary code execution on an affected device.nThe	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35483	A-HMT-DAVI-070820/257

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is due to a stack overflow read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device. **CVE ID : CVE-2020-7816**		
hylafax\+_project					
hylafax\+					
Improper Privilege Management	30-06-2020	7.2	In HylaFAX+ through 7.0.2 and HylaFAX Enterprise, the faxsetup utility calls chown on files in user-owned directories. By winning a race, a local attacker could use this to escalate his privileges to root. **CVE ID : CVE-2020-15396**	N/A	A-HYL-HYLA-070820/258
Improper Privilege Management	30-06-2020	7.2	HylaFAX+ through 7.0.2 and HylaFAX Enterprise have scripts that execute binaries from directories writable by unprivileged users (e.g., locations under /var/spool/hylafax that are writable by the uucp account). This allows these users to execute code in the context of the user calling these binaries (often root). **CVE ID : CVE-2020-15397**	N/A	A-HYL-HYLA-070820/259
ibi					
webfocus_business_intelligence					
Improper Neutralization of Input During Web Page	22-06-2020	4.3	WebFOCUS Business Intelligence 8.0 (SP6) was prone to XSS via arbitrary URL parameters.	N/A	A-IBI-WEBF-070820/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2020-14202**		
Cross-Site Request Forgery (CSRF)	22-06-2020	6.8	WebFOCUS Business Intelligence 8.0 (SP6) allows a Cross-Site Request Forgery (CSRF) attack against administrative users within the /ibi_apps/WFServlet(.ibfs) endpoint. The impact may be creation of an administrative user. It can also be exploited in conjunction with CVE-2016-9044. **CVE ID : CVE-2020-14203**	N/A	A-IBI-WEBF-070820/261
Improper Restriction of XML External Entity Reference ('XXE')	22-06-2020	5.8	In WebFOCUS Business Intelligence 8.0 (SP6), the administration portal allows remote attackers to read arbitrary local files or forge server-side HTTP requests via a crafted HTTP request to /ibi_apps/WFServlet.cfg because XML external entity injection is possible. This is related to making changes to the application repository configuration. **CVE ID : CVE-2020-14204**	N/A	A-IBI-WEBF-070820/262
IBM					
security_guardium					
Use of Insufficiently Random Values	23-06-2020	5	IBM Security Guardium 10.6 and 11.1 may use insufficiently random numbers or values in a security context that depends on unpredictable numbers. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6237074	A-IBM-SECU-070820/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			174807. **CVE ID : CVE-2020-4188**		
spectrum_protect_plus					
Information Exposure	26-06-2020	4.3	IBM Spectrum Protect Plus 10.1.0 through 10.1.5 could allow an attacker to obtain sensitive information due to insecure communications being used between the application and server. IBM X-Force ID: 183935. **CVE ID : CVE-2020-4565**	https://www.ibm.com/support/pages/node/6238920	A-IBM-SPEC-070820/264
websphere_mq					
N/A	16-06-2020	5	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081. **CVE ID : CVE-2020-4310**	https://www.ibm.com/support/pages/node/6223914	A-IBM-WEBS-070820/265
doors_next					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2020	3.5	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176141. **CVE ID : CVE-2020-4281**	https://www.ibm.com/support/pages/node/6235162	A-IBM-DOOR-070820/266
Improper Neutralizatio	19-06-2020	3.5	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6,	https://www.ibm.com/	A-IBM-DOOR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176408. **CVE ID : CVE-2020-4295**	support/pages/node/6235162	070820/267
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2020	3.5	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176474. **CVE ID : CVE-2020-4297**	https://www.ibm.com/support/pages/node/6235162	A-IBM-DOOR-070820/268
security_secret_server					
Improper Restriction of Rendered UI Layers or Frames	24-06-2020	4.3	IBM Security Secret Server 10.7 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID:	https://www.ibm.com/support/pages/node/6237266	A-IBM-SECU-070820/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			177511. **CVE ID : CVE-2020-4322**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	4.3	IBM Security Secret Server 10.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 177514. **CVE ID : CVE-2020-4323**	https://www.ibm.com/support/pages/node/6237286	A-IBM-SECU-070820/270
Information Exposure Through an Error Message	24-06-2020	5	IBM Security Secret Server 10.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 177599. **CVE ID : CVE-2020-4327**	https://www.ibm.com/support/pages/node/6237260	A-IBM-SECU-070820/271
Information Exposure Through an Error Message	24-06-2020	5	IBM Security Secret Server 10.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 178181. **CVE ID : CVE-2020-4341**	https://www.ibm.com/support/pages/node/6237084	A-IBM-SECU-070820/272
Information	24-06-2020	5	IBM Security Secret Server 10.7 could disclose sensitive	https://www.ibm.com/	A-IBM-SECU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			information included in installation files to an unauthorized user. IBM X-Force ID: 178182. **CVE ID : CVE-2020-4342**	support/pages/node/6237276	070820/273
Information Exposure	24-06-2020	4.3	IBM Security Secret Server 10.7 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 179988. **CVE ID : CVE-2020-4413**	https://www.ibm.com/support/pages/node/6237292	A-IBM-SECU-070820/274
api_connect					
Information Exposure	29-06-2020	5	IBM API Connect V2018.4.1.0 through 2018.4.1.11 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 181324. **CVE ID : CVE-2020-4452**	https://www.ibm.com/support/pages/node/6240322	A-IBM-API_-070820/275
maximo_asset_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-06-2020	3.5	IBM Maximo Asset Management 7.6.0.10 and 7.6.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials	https://www.ibm.com/support/pages/node/6238376	A-IBM-MAXI-070820/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure within a trusted session. IBM X-Force ID: 175121. **CVE ID : CVE-2020-4223**		
mq					
N/A	16-06-2020	5	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081. **CVE ID : CVE-2020-4310**	https://www.ibm.com/support/pages/node/6223914	A-IBM-MQ-070820/277
Improper Certificate Validation	16-06-2020	4	IBM MQ Appliance and IBM MQ AMQP Channels 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD do not correctly block or allow clients based on the certificate distinguished name SSLPEER setting. IBM X-Force ID: 177403. **CVE ID : CVE-2020-4320**	https://www.ibm.com/support/pages/node/5736885	A-IBM-MQ-070820/278
rational_doors_next_generation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2020	3.5	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176141. **CVE ID : CVE-2020-4281**	https://www.ibm.com/support/pages/node/6235162	A-IBM-RATI-070820/279
Improper	19-06-2020	3.5	IBM DOORS Next Generation	https://ww	A-IBM-RATI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			(DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176408. **CVE ID : CVE-2020-4295**	w.ibm.com/support/pages/node/6235162	070820/280
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2020	3.5	IBM DOORS Next Generation (DNG/RRC) 6.0.2, 6.0.6, 6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 176474. **CVE ID : CVE-2020-4297**	https://www.ibm.com/support/pages/node/6235162	A-IBM-RATI-070820/281
business_automation_workflow					
Information Exposure	17-06-2020	5	IBM Business Automation Workflow and IBM Business Process Manager (IBM Business Process Manager Express 8.5.5, 8.5.6, 8.5.7, and 8.6) could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further	https://www.ibm.com/support/pages/node/6233276	A-IBM-BUSI-070820/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacks against the system. IBM X-Force ID: 182716. **CVE ID : CVE-2020-4532**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-06-2020	3.5	IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 183611. **CVE ID : CVE-2020-4557**	https://www.ibm.com/support/pages/node/6241338	A-IBM-BUSI-070820/283
business_process_manager					
Information Exposure	17-06-2020	5	IBM Business Automation Workflow and IBM Business Process Manager (IBM Business Process Manager Express 8.5.5, 8.5.6, 8.5.7, and 8.6) could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 182716. **CVE ID : CVE-2020-4532**	https://www.ibm.com/support/pages/node/6233276	A-IBM-BUSI-070820/284
Improper Neutralization of Input During Web Page	29-06-2020	3.5	IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 are vulnerable to cross-site	https://www.ibm.com/support/pages/node/6241338	A-IBM-BUSI-070820/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 183611. **CVE ID : CVE-2020-4557**		
idrive					
idrive					
Incorrect Default Permissions	26-06-2020	7.2	IDrive before 6.7.3.19 on Windows installs by default to %PROGRAMFILES(X86)%\IDriveWindows with weak folder permissions granting any user modify permission (i.e., NT AUTHORITY\Authenticated Users:(OI)(CI)(M)) to the contents of the directory and its sub-folders. In addition, the program installs a service called IDriveService that runs as LocalSystem. Thus, any standard user can escalate privileges to NT AUTHORITY\SYSTEM by substituting the service's binary with a malicious one. **CVE ID : CVE-2020-15351**	N/A	A-IDR-IDRI-070820/286
idsoftware					
tech_1					
Buffer Copy without Checking Size of Input	24-06-2020	7.5	A buffer overflow in the M_LoadDefaults function in m_misc.c in id Tech 1 (aka Doom engine) allows	N/A	A-IDS-TECH-070820/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			arbitrary code execution via an unsafe usage of fscanf, because it does not limit the number of characters to be read in a format argument. **CVE ID : CVE-2020-15007**		
ifax					
hylafax_enterprise					
Improper Privilege Management	30-06-2020	7.2	In HylaFAX+ through 7.0.2 and HylaFAX Enterprise, the faxsetup utility calls chown on files in user-owned directories. By winning a race, a local attacker could use this to escalate his privileges to root. **CVE ID : CVE-2020-15396**	N/A	A-IFA-HYLA-070820/288
Improper Privilege Management	30-06-2020	7.2	HylaFAX+ through 7.0.2 and HylaFAX Enterprise have scripts that execute binaries from directories writable by unprivileged users (e.g., locations under /var/spool/hylafax that are writable by the uucp account). This allows these users to execute code in the context of the user calling these binaries (often root). **CVE ID : CVE-2020-15397**	N/A	A-IFA-HYLA-070820/289
Iobit					
advanced_systemcare					
Improper Privilege Management	22-06-2020	3.6	IOBit Advanced SystemCare Free 13.5.0.263 allows local users to gain privileges for file deletion by manipulating the Clean & Optimize feature with an NTFS junction and	N/A	A-IOB-ADVA-070820/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an Object Manager symbolic link. **CVE ID : CVE-2020-14990**		
malware_fighter					
Improper Link Resolution Before File Access ('Link Following')	30-06-2020	2.1	IOBit Malware Fighter Pro 8.0.2.547 allows local users to gain privileges for file deletion by manipulating malicious flagged file locations with an NTFS junction and an Object Manager symbolic link. **CVE ID : CVE-2020-15401**	N/A	A-IOB-MALW-070820/291
iobit_unlocker					
Improper Privilege Management	23-06-2020	6.6	The driver in IOBit Unlocker 1.1.2 allows a low-privileged user to unlock a file and kill processes (even ones running as SYSTEM) that hold a handle, via IOCTL code 0x222124. **CVE ID : CVE-2020-14974**	N/A	A-IOB-IOBI-070820/292
Improper Privilege Management	23-06-2020	7.2	The driver in IOBit Unlocker 1.1.2 allows a low-privileged user to delete, move, or copy arbitrary files via IOCTL code 0x222124. **CVE ID : CVE-2020-14975**	N/A	A-IOB-IOBI-070820/293
ISC					
bind					
Reachable Assertion	17-06-2020	4	An attacker who is permitted to send zone data to a server via zone transfer can exploit this to intentionally trigger the assertion failure with a specially constructed zone, denying service to clients.	https://kb.isc.org/docs/cve-2020-8618, https://security.netapp.com/advi	A-ISC-BIND-070820/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8618	sory/ntap-20200625-0003/	
Improper Resource Shutdown or Release	17-06-2020	4	In ISC BIND9 versions BIND 9.11.14 -> 9.11.19, BIND 9.14.9 -> 9.14.12, BIND 9.16.0 -> 9.16.3, BIND Supported Preview Edition 9.11.14-S1 -> 9.11.19-S1: Unless a nameserver is providing authoritative service for one or more zones and at least one zone contains an empty non-terminal entry containing an asterisk ("*") character, this defect cannot be encountered. A would-be attacker who is allowed to change zone content could theoretically introduce such a record in order to exploit this condition to cause denial of service, though we consider the use of this vector unlikely because any such attack would require a significant privilege level and be easily traceable. **CVE ID : CVE-2020-8619**	https://kb.isc.org/docs/cve-2020-8619, https://security.netapp.com/advisory/ntap-20200625-0003/	A-ISC-BIND-070820/295
jhipster					
generator-jhipster-kotlin					
Improper Output Neutralization for Logs	25-06-2020	5	In generator-jhipster-kotlin version 1.6.0 log entries are created for invalid password reset attempts. As the email is provided by a user and the api is public this can be used by an attacker to forge log entries. This is vulnerable to	https://github.com/jhipster/jhipster-kotlin/security/advisories/GHSA-pfxf-wh96-	A-JHI-GENE-070820/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			https://cwe.mitre.org/data/definitions/117.html This problem affects only application generated with jwt or session authentication. Applications using oauth are not vulnerable. This issue has been fixed in version 1.7.0. **CVE ID : CVE-2020-4072**	fvjc	
Jiangmin					
jiangmin_antivirus					
Uncontrolled Resource Consumption	26-06-2020	4.9	In Jiangmin Antivirus 16.0.13.129, the driver file (KVFG.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x220440. **CVE ID : CVE-2020-14955**	N/A	A-JIA-JIAN-070820/297
jsrsasign_project					
jsrsasign					
Improper Verification of Cryptographic Signature	22-06-2020	5	An issue was discovered in the jsrsasign package through 8.0.18 for Node.js. It allows a malleability in ECDSA signatures by not checking overflows in the length of a sequence and '0' characters appended or prepended to an integer. The modified signatures are verified as valid. This could have a security-relevant impact if an application relied on a single canonical	N/A	A-JSR-JSRS-070820/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signature. **CVE ID : CVE-2020-14966**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-06-2020	7.5	An issue was discovered in the jsrsasign package before 8.0.18 for Node.js. Its RSA PKCS1 v1.5 decryption implementation does not detect ciphertext modification by prepending '\0' bytes to ciphertexts (it decrypts modified ciphertexts without error). An attacker might prepend these bytes with the goal of triggering memory corruption issues. **CVE ID : CVE-2020-14967**	N/A	A-JSR-JSRS-070820/299
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-06-2020	7.5	An issue was discovered in the jsrsasign package before 8.0.17 for Node.js. Its RSASSA-PSS (RSA-PSS) implementation does not detect signature manipulation/modification by prepending '\0' bytes to a signature (it accepts these modified signatures as valid). An attacker can abuse this behavior in an application by creating multiple valid signatures where only one signature should exist. Also, an attacker might prepend these bytes with the goal of triggering memory corruption issues. **CVE ID : CVE-2020-14968**	N/A	A-JSR-JSRS-070820/300
kordil_edms_project					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
kordil_edms					
Unrestricted Upload of File with Dangerous Type	22-06-2020	6.5	documents_add.php in Kordil EDMS through 2.2.60rc3 allows Remote Command Execution because .php files can be uploaded to the documents folder. **CVE ID : CVE-2020-13887**	N/A	A-KOR-KORD-070820/301
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	3.5	Kordil EDMS through 2.2.60rc3 allows stored XSS in users_edit.php, users_management_edit.php, and user_management.php. **CVE ID : CVE-2020-13888**	N/A	A-KOR-KORD-070820/302
Libraw					
libraw					
Out-of-bounds Write	28-06-2020	4.3	LibRaw before 0.20-Beta3 has an out-of-bounds write in parse_exif() in metadata\exif_gps.cpp via an unrecognized AtomName and a zero value of tiff_nifds. **CVE ID : CVE-2020-15365**	N/A	A-LIB-LIBR-070820/303
libvncserver_project					
libvncserver					
NULL Pointer Dereference	17-06-2020	5	An issue was discovered in LibVNCServer before 0.9.13. libvncclient/tls_openssl.c has a NULL pointer dereference. **CVE ID : CVE-2020-14396**	N/A	A-LIB-LIBV-070820/304
NULL Pointer Dereference	17-06-2020	5	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rfbregion.c has	N/A	A-LIB-LIBV-070820/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a NULL pointer dereference. **CVE ID : CVE-2020-14397**		
Loop with Unreachable Exit Condition ('Infinite Loop')	17-06-2020	5	An issue was discovered in LibVNCServer before 0.9.13. An improperly closed TCP connection causes an infinite loop in libvncclient/sockets.c. **CVE ID : CVE-2020-14398**	N/A	A-LIB-LIBV-070820/306
N/A	17-06-2020	5	An issue was discovered in LibVNCServer before 0.9.13. Byte-aligned data is accessed through uint32_t pointers in libvncclient/rfbproto.c. **CVE ID : CVE-2020-14399**	N/A	A-LIB-LIBV-070820/307
N/A	17-06-2020	5	An issue was discovered in LibVNCServer before 0.9.13. Byte-aligned data is accessed through uint16_t pointers in libvncserver/translate.c. **CVE ID : CVE-2020-14400**	N/A	A-LIB-LIBV-070820/308
Integer Overflow or Wraparound	17-06-2020	7.5	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/scale.c has a pixel_value integer overflow. **CVE ID : CVE-2020-14401**	N/A	A-LIB-LIBV-070820/309
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-06-2020	7.5	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/corre.c allows out-of-bounds access via encodings. **CVE ID : CVE-2020-14402**	N/A	A-LIB-LIBV-070820/310
Improper Restriction of Operations	17-06-2020	7.5	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/hextile.c allows out-of-bounds access via	N/A	A-LIB-LIBV-070820/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			encodings. **CVE ID : CVE-2020-14403**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-06-2020	7.5	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rre.c allows out-of-bounds access via encodings. **CVE ID : CVE-2020-14404**	N/A	A-LIB-LIBV-070820/312
Allocation of Resources Without Limits or Throttling	17-06-2020	7.5	An issue was discovered in LibVNCServer before 0.9.13. libvncclient/rfbproto.c does not limit TextChat size. **CVE ID : CVE-2020-14405**	N/A	A-LIB-LIBV-070820/313
limdu_project					
limdu					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-06-2020	9	In Limdu before 0.95, the trainBatch function has a command injection vulnerability. Clients of the Limdu library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. This has been patched in 0.95. **CVE ID : CVE-2020-4066**	https://github.com/erelsgl/limdu/security/advisories/GHSA-77qv-gh6f-pgh4	A-LIM-LIMD-070820/314
Linuxfoundation					
ceph					
Incorrect Authorization	22-06-2020	5.2	An authorization bypass vulnerability was found in Ceph versions 15.2.0 before 15.2.2, where the ceph-mon and ceph-mgr daemons do not properly restrict access,	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10736	A-LIN-CEPH-070820/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in gaining access to unauthorized resources. This flaw allows an authenticated client to modify the configuration and possibly conduct further attacks. **CVE ID : CVE-2020-10736**		
jaeger					
Information Exposure Through Log Files	19-06-2020	2.1	Sensitive information written to a log file vulnerability was found in jaegertracing/jaeger before version 1.18.1 when the Kafka data store is used. This flaw allows an attacker with access to the container's log file to discover the Kafka credentials. **CVE ID : CVE-2020-10750**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10750, https://github.com/jaegertracing/jaeger/releases/tag/v1.18.1	A-LIN-JAEG-070820/316
machothemes					
image_photo_gallery_final_tiles_grid					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	3.5	Multiple XSS vulnerabilities in the Final Tiles Gallery plugin before 3.4.19 for WordPress allow remote attackers to inject arbitrary web script or HTML via the Title (aka imageTitle) or Caption (aka description) field of an image to wp-admin/admin-ajax.php. **CVE ID : CVE-2020-14962**	N/A	A-MAC-IMAG-070820/317
mageme					
webforms_pro_m2					
Improper Neutralizatio	29-06-2020	4.3	XSS exists in the WebForms Pro M2 extension before	N/A	A-MAG-WEBF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			2.9.17 for Magento 2 via the textarea field. **CVE ID : CVE-2020-12635**		070820/318
Magento					
magento					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9576**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/319
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-06-2020	4.3	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure . **CVE ID : CVE-2020-9577**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/320
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9578**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9579**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/322
N/A	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9580**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/323
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-06-2020	4.3	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2020-9581**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/324
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/325

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9582		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9583**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/326
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-06-2020	3.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a stored cross-site scripting vulnerability. Successful exploitation could lead to sensitive information disclosure. **CVE ID : CVE-2020-9584**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/327
N/A	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9585**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/328
Incorrect Authorization	26-06-2020	5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an authorization bypass vulnerability. Successful exploitation could lead to potentially	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/329

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized product discounts. **CVE ID : CVE-2020-9587**		
Information Exposure Through Discrepancy	26-06-2020	6.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have an observable timing discrepancy vulnerability. Successful exploitation could lead to signature verification bypass. **CVE ID : CVE-2020-9588**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/330
Information Exposure	26-06-2020	5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a defense-in-depth security mitigation vulnerability. Successful exploitation could lead to unauthorized access to admin panel. **CVE ID : CVE-2020-9591**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/331
Improper Privilege Management	26-06-2020	7.5	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a business logic error vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9630**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/332
N/A	26-06-2020	10	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security	https://helpx.adobe.com/security/products/magento/a	A-MAG-MAGE-070820/333

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9631**	psb20-22.html	
N/A	26-06-2020	10	Magento versions 2.3.4 and earlier, 2.2.11 and earlier (see note), 1.14.4.4 and earlier, and 1.9.4.4 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9632**	https://helpx.adobe.com/security/products/magento/apsb20-22.html	A-MAG-MAGE-070820/334
mattermost					
mattermost_server					
Loop with Unreachable Exit Condition ('Infinite Loop')	19-06-2020	5	An issue was discovered in Mattermost Server before 5.23.0. Large webhook requests allow attackers to cause a denial of service (infinite loop), aka MMSA-2020-0021. **CVE ID : CVE-2020-14447**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/335
Loop with Unreachable Exit Condition ('Infinite Loop')	19-06-2020	5	An issue was discovered in Mattermost Server before 5.23.0. Automatic direct message replies allow attackers to cause a denial of service (infinite loop), aka MMSA-2020-0020. **CVE ID : CVE-2020-14448**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/336
N/A	19-06-2020	5	An issue was discovered in Mattermost Server before 5.22.0. The markdown renderer allows attackers to cause a denial of service	https://mattermost.com/security-updates/	A-MAT-MATT-070820/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(client-side), aka MMSA-2020-0017. **CVE ID : CVE-2020-14450**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-06-2020	5	An issue was discovered in Mattermost Server before 5.21.0. mmctl allows directory traversal via HTTP, aka MMSA-2020-0014. **CVE ID : CVE-2020-14452**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/338
Insufficient Verification of Data Authenticity	19-06-2020	5	An issue was discovered in Mattermost Server before 5.21.0. Socket read operations are not appropriately restricted, which allows attackers to cause a denial of service, aka MMSA-2020-0005. **CVE ID : CVE-2020-14453**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/339
Missing Authorization	19-06-2020	5	An issue was discovered in Mattermost Server before 5.20.0. Non-members can receive broadcasted team details via the update_team WebSocket event, aka MMSA-2020-0012. **CVE ID : CVE-2020-14457**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/340
Information Exposure	19-06-2020	5	An issue was discovered in Mattermost Server before 5.19.0. Attackers can discover private channels via the "get channel by name" API, aka MMSA-2020-0004. **CVE ID : CVE-2020-14458**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/341
Improper Input Validation	19-06-2020	5	An issue was discovered in Mattermost Server before 5.19.0. Attackers can rename	https://mattermost.com/security-	A-MAT-MATT-070820/342

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a channel and cause a collision with a direct message, aka MMSA-2020-0002. **CVE ID : CVE-2020-14459**	updates/	
Improper Privilege Management	19-06-2020	4	An issue was discovered in Mattermost Server before 5.19.0, 5.18.1, 5.17.3, 5.16.5, and 5.9.8. Creation of a trusted OAuth application does not always require admin privileges, aka MMSA-2020-0001. **CVE ID : CVE-2020-14460**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/343
mattermost_mobile					
Information Exposure	19-06-2020	4.3	An issue was discovered in Mattermost Mobile Apps before 1.30.0. Authorization tokens can sometimes be disclosed to third-party servers, aka MMSA-2020-0018. **CVE ID : CVE-2020-14449**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/344
Information Exposure	19-06-2020	5	An issue was discovered in Mattermost Mobile Apps before 1.29.0. The iOS app allowed Single Sign-On cookies and Local Storage to remain after a logout, aka MMSA-2020-0013. **CVE ID : CVE-2020-14451**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/345
mattermost_desktop					
URL Redirection to Untrusted Site ('Open Redirect')	19-06-2020	5.8	An issue was discovered in Mattermost Desktop App before 4.4.0. Attackers can open web pages in the desktop application because server redirection is	https://mattermost.com/security-updates/	A-MAT-MATT-070820/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mishandled, aka MMSA-2020-0008. **CVE ID : CVE-2020-14454**		
Improper Authentication	19-06-2020	4.3	An issue was discovered in Mattermost Desktop App before 4.4.0. Prompting for HTTP Basic Authentication is mishandled, allowing phishing, aka MMSA-2020-0007. **CVE ID : CVE-2020-14455**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/347
Origin Validation Error	19-06-2020	7.5	An issue was discovered in Mattermost Desktop App before 4.4.0. The Same Origin Policy is mishandled during access-control decisions for web APIs, aka MMSA-2020-0006. **CVE ID : CVE-2020-14456**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/348
mattermost					
Information Exposure	26-06-2020	5	An issue was discovered in Mattermost Mobile Apps before 1.31.2 on iOS. Unintended third-party servers could sometimes obtain authorization tokens, aka MMSA-2020-0022. **CVE ID : CVE-2020-13891**	https://mattermost.com/security-updates/	A-MAT-MATT-070820/349
Mcafee					
advanced_threat_defense					
Information Exposure	22-06-2020	2.1	Improper Access Control vulnerability in McAfee Advanced Threat Defense (ATD) prior to 4.10.0 allows local users to view sensitive files via a carefully crafted HTTP request parameter.	https://kc.mcafee.com/corporate/index?page=content&id=SB10319	A-MCA-ADVA-070820/350

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7262		
mediaarea					
mediainfo					
Out-of-bounds Read	30-06-2020	6.8	In MediaInfoLib in MediaArea MediaInfo 20.03, there is a stack-based buffer over-read in Streams_Fill_PerStream in Multiple/File_MpegPs.cpp (aka an off-by-one during MpegPs parsing). **CVE ID : CVE-2020-15395**	N/A	A-MED-MEDI-070820/351
Mediawiki					
mediawiki					
Information Exposure	24-06-2020	2.6	In MediaWiki before 1.31.8, 1.32.x and 1.33.x before 1.33.4, and 1.34.x before 1.34.2, private wikis behind a caching server using the img_auth.php image authorization security feature may have had their files cached publicly, so any unauthorized user could view them. This occurs because Cache-Control and Vary headers were mishandled. **CVE ID : CVE-2020-15005**	https://gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/core/+/REL1_31/RELEASE-NOTES-1.31, https://gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/core/+/REL1_33/RELEASE-NOTES-1.33, https://lists.wikimedia.org/pipermail/wikitech-l/2020-	A-MED-MEDI-070820/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				June/093535.html	
Microfocus					
arcsight_management_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-06-2020	3.5	Cross Site Scripting (XSS) vulnerability in Micro Focus ArcSight Management Center product, Affecting versions 2.6.1, 2.7.x, 2.8.x, 2.9.x prior to 2.9.4. The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS) or information disclosure. **CVE ID : CVE-2020-11838**	N/A	A-MIC-ARCS-070820/353
Information Exposure	16-06-2020	4	Unauthorized information disclosure vulnerability in Micro Focus ArcSight Management Center product, Affecting versions 2.6.1, 2.7.x, 2.8.x, 2.9.x prior to 2.9.4. The vulnerabilities could be remotely exploited resulting unauthorized information disclosure. **CVE ID : CVE-2020-11840**	N/A	A-MIC-ARCS-070820/354
Information Exposure	16-06-2020	4	Unauthorized information disclosure vulnerability in Micro Focus ArcSight Management Center product, Affecting versions 2.6.1, 2.7.x, 2.8.x, 2.9.x prior to 2.9.4. The vulnerabilities could be remotely exploited resulting unauthorized information disclosure. **CVE ID : CVE-2020-11841**	N/A	A-MIC-ARCS-070820/355
arcsight_enterprise_security_manager_express					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-06-2020	4.3	Cross Site Scripting (XSS) vulnerability in Micro Focus ArcSight Enterprise Security Manager (ESM) product, Affecting versions 7.0.x, 7.2 and 7.2.1 . The vulnerabilities could be remotely exploited resulting in Cross-Site Scripting (XSS) or information disclosure. **CVE ID : CVE-2020-9522**	N/A	A-MIC-ARCS-070820/356
Misp					
misp					
Improper Privilege Management	30-06-2020	7.5	An issue was discovered in MISP 2.4.128. app/Controller/AttributesController.php has insufficient ACL checks in the attachment downloader. **CVE ID : CVE-2020-15411**	N/A	A-MIS-MISP-070820/357
Information Exposure	22-06-2020	5	app/Model/Attribute.php in MISP 2.4.127 lacks an ACL lookup on attribute correlations. This occurs when querying the attribute restsearch API, revealing metadata about a correlating but unreachable attribute. **CVE ID : CVE-2020-14969**	N/A	A-MIS-MISP-070820/358
Improper Privilege Management	30-06-2020	4	An issue was discovered in MISP 2.4.128. app/Controller/EventsController.php lacks an event ACL check before proceeding to allow a user to send an event contact form. **CVE ID : CVE-2020-15412**	N/A	A-MIS-MISP-070820/359
Mitre					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
caldera					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	19-06-2020	3.5	CALDERA 2.7.0 allows XSS via the Operation Name box. **CVE ID : CVE-2020-14462**	N/A	A-MIT-CALD-070820/360
Mitsubishielectric					
cpu_module_logging_configuration_tool					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator	N/A	A-MIT-CPU_-070820/361

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier,	N/A	A-MIT-CPU_-070820/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
cw_configurator					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier,	N/A	A-MIT-CW_C-070820/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and	N/A	A-MIT-CW_C-070820/364

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
em_configurator					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L	N/A	A-MIT-EM_C-070820/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver.	N/A	A-MIT-EM_C-070820/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gt_designer3					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to	N/A	A-MIT-GT_D-070820/367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT	N/A	A-MIT-GT_D-070820/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
gx_logviewer					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI	N/A	A-MIT-GX_L-070820/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT	N/A	A-MIT-GX_L-070820/370

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
gx_works2					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and	N/A	A-MIT-GX_W-070820/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver.	N/A	A-MIT-GX_W-070820/372

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
gx_works3					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3	N/A	A-MIT-GX_W-070820/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW	N/A	A-MIT-GX_W-070820/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
m_commdtm-hart					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity	N/A	A-MIT-M_CO-070820/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and	N/A	A-MIT-M_CO-070820/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
m_commdtm-io-link					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D	N/A	A-MIT-M_CO-070820/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver.	N/A	A-MIT-M_CO-070820/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
melfa-works					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible	N/A	A-MIT-MELF-070820/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier,	N/A	A-MIT-MELF-070820/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
melsec-l_flexible_high-speed_i\/o_control_module_configuration_tool					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and	N/A	A-MIT-MELS-070820/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and	N/A	A-MIT-MELS-070820/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
melsoft_fielddeviceconfigurator					
Improper	30-06-2020	5	Mitsubishi Electoric FA	N/A	A-MIT-MELS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of XML External Entity Reference ('XXE')			Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified		070820/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver.	N/A	A-MIT-MELS-070820/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
melsoft_iq_appportal					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control	N/A	A-MIT-MELS-070820/385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT	N/A	A-MIT-MELS-070820/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
melsoft_navigator					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control	N/A	A-MIT-MELS-070820/387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver.	N/A	A-MIT-MELS-070820/388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
mi_configurator					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver.	N/A	A-MIT-MI_C-070820/389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software	N/A	A-MIT-MI_C-070820/390

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
motion_control_setting					
Improper Restriction	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU	N/A	A-MIT-MOTI-070820/391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of XML External Entity Reference ('XXE')			Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors.		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5602		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT	N/A	A-MIT-MOTI-070820/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
mr_configurator2					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and	N/A	A-MIT-MR_C-070820/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and	N/A	A-MIT-MR_C-070820/394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
mt_works2					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool	N/A	A-MIT-MT_W-070820/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-	N/A	A-MIT-MT_W-070820/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
rt_toolbox2					
Improper Restriction of XML External Entity Reference ('XXE')	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX	N/A	A-MIT-RT_T-070820/397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM	N/A	A-MIT-RT_T-070820/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
rt_toolbox3					
Improper Restriction of XML	30-06-2020	5	Mitsubishi Electoric FA Engineering Software (CPU Module Logging	N/A	A-MIT-RT_T-070820/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference ('XXE')			Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and earlier) allows an attacker to conduct XML External Entity (XXE) attacks via unspecified vectors. **CVE ID : CVE-2020-5602**		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	30-06-2020	5	Uncontrolled resource consumption vulnerability in Mitsubishi Electoric FA Engineering Software (CPU Module Logging Configuration Tool Ver. 1.94Y and earlier, CW Configurator Ver. 1.010L and earlier, EM Software Development Kit (EM Configurator) Ver. 1.010L and earlier, GT Designer3 (GOT2000) Ver. 1.221F and earlier, GX LogViewer Ver. 1.96A and earlier, GX Works2 Ver. 1.586L and earlier, GX Works3 Ver. 1.058L and earlier, M_CommDTM-HART Ver. 1.00A, M_CommDTM-IO-Link Ver. 1.02C and earlier, MELFA-Works Ver. 4.3 and earlier, MELSEC-L Flexible High-Speed I/O Control Module Configuration Tool Ver.1.004E and earlier, MELSOFT FieldDeviceConfigurator Ver. 1.03D and earlier, MELSOFT iQ AppPortal Ver. 1.11M and earlier, MELSOFT Navigator Ver. 2.58L and earlier, MI Configurator Ver. 1.003D and earlier, Motion Control Setting Ver. 1.005F and earlier, MR Configurator2 Ver. 1.72A and earlier, MT Works2 Ver. 1.156N and earlier, RT ToolBox2 Ver. 3.72A and earlier, and RT ToolBox3 Ver. 1.50C and	N/A	A-MIT-RT_T-070820/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier) allows an attacker to cause a denial of service (DoS) condition attacks via unspecified vectors. **CVE ID : CVE-2020-5603**		
mjml					
mjml					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-06-2020	6.4	MJML prior to 4.6.3 contains a path traversal vulnerability when processing the mj-include directive within an MJML document. **CVE ID : CVE-2020-12827**	N/A	A-MJM-MJML-070820/401
mk-auth					
mk-auth					
Improper Authenticati on	29-06-2020	7.5	An issue was discovered in MK-AUTH 19.01. The web login functionality allows an attacker to bypass authentication and gain client privileges via SQL injection in central/executar_login.php. **CVE ID : CVE-2020-14068**	N/A	A-MK--MK-A-070820/402
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	29-06-2020	4.6	An issue was discovered in MK-AUTH 19.01. There are SQL injection issues in mkt/ PHP scripts, as demonstrated by arp.php, dhcp.php, hotspot.php, ip.php, pgaviso.php, pgcorte.php, pppoe.php, queues.php, and wifi.php. **CVE ID : CVE-2020-14069**	N/A	A-MK--MK-A-070820/403
Use of Hard-coded	29-06-2020	10	An issue was discovered in MK-AUTH 19.01. There is	N/A	A-MK--MK-A-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			authentication bypass in the web login functionality because guessable credentials to admin/executar_login.php result in admin access. **CVE ID : CVE-2020-14070**		070820/404
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-06-2020	4.3	An issue was discovered in MK-AUTH 19.01. XSS vulnerabilities in admin and client scripts allow an attacker to execute arbitrary JavaScript code. **CVE ID : CVE-2020-14071**	N/A	A-MK--MK-A-070820/405
N/A	29-06-2020	10	An issue was discovered in MK-AUTH 19.01. It allows command execution as root via shell metacharacters to /auth admin scripts. **CVE ID : CVE-2020-14072**	N/A	A-MK--MK-A-070820/406
monitorapp					
application_insight_web_application					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-06-2020	4.3	MONITORAPP AIWAF-VE and AIWAF-4000 through 2020-06-16 allow reflected Cross-Site Scripting (XSS) through a crafted URL. This occurs because the Detect URL field displays the original URL. **CVE ID : CVE-2020-14210**	N/A	A-MON-APPL-070820/407
web_application_firewall					
Improper Neutralization of Input During Web Page	16-06-2020	4.3	MONITORAPP AIWAF-VE and AIWAF-4000 through 2020-06-16 allow reflected Cross-Site Scripting (XSS) through a crafted URL. This	N/A	A-MON-WEB_-070820/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			occurs because the Detect URL field displays the original URL. **CVE ID : CVE-2020-14210**		
Mutt					
mutt					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	21-06-2020	4.3	Mutt before 1.14.4 and NeoMutt before 2020-06-19 have a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a man-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-14954**	N/A	A-MUT-MUTT-070820/409
mversion_project					
mversion					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-06-2020	7.5	In mversion before 2.0.0, there is a command injection vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. This vulnerability is patched by version 2.0.0. Previous releases are deprecated in npm. As a workaround, make sure to escape git commit messages when using the commitMessage option for the update function. **CVE ID : CVE-2020-4059**	https://github.com/mikaelbr/mversion/security/advisories/GHSA-qjg4-w4c6-f6c6	A-MVE-MVER-070820/410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
naviwebs					
navigate_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	4.3	An issue was discovered in Navigate CMS 2.9 r1433. There is a stored XSS vulnerability that is executed on the page to view users, and on the page to edit users. This is present in both the User field and the E-Mail field. On the Edit user page, the XSS is only triggered via the E-Mail field; however, on the View user page the XSS is triggered via either the User field or the E-Mail field. **CVE ID : CVE-2020-14018**	N/A	A-NAV-NAVI-070820/411
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	An issue was discovered in Navigate CMS 2.9 r1433. The query parameter fid on the resource navigate.php does not perform sufficient data validation and/or encoding, making it vulnerable to reflected XSS. **CVE ID : CVE-2020-14014**	N/A	A-NAV-NAVI-070820/412
Weak Password Recovery Mechanism for Forgotten Password	24-06-2020	5	An issue was discovered in Navigate CMS 2.9 r1433. When performing a password reset, a user is emailed an activation code that allows them to reset their password. There is, however, a flaw when no activation code is supplied. The system will allow an unauthorized user to continue setting a password, even though no activation	N/A	A-NAV-NAVI-070820/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code was supplied, setting the password for the most recently created user in the system (the user with the highest user id). **CVE ID : CVE-2020-14015**		
Weak Password Recovery Mechanism for Forgotten Password	24-06-2020	5	An issue was discovered in Navigate CMS 2.9 r1433. The forgot-password feature allows users to reset their passwords by using either their username or the email address associated with their account. However, the feature returns a not_found message when the provided username or email address does not match a user in the system. This can be used to enumerate users. **CVE ID : CVE-2020-14016**	N/A	A-NAV-NAVI-070820/414
Cleartext Storage of Sensitive Information	24-06-2020	5	An issue was discovered in Navigate CMS 2.9 r1433. Sessions, as well as associated information such as CSRF tokens, are stored in cleartext files in the directory /private/sessions. An unauthenticated user could use a brute-force approach to attempt to identify existing sessions, or view the contents of this file to discover details about a session. **CVE ID : CVE-2020-14017**	N/A	A-NAV-NAVI-070820/415
Improper Neutralization of Input	19-06-2020	3.5	Navigate CMS 2.9 allows XSS via the Alias or Real URL field of the "Web Sites >	N/A	A-NAV-NAVI-070820/416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Create > Aliases > Add" screen. **CVE ID : CVE-2020-14927**		
nedi					
nedi					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-06-2020	9	NeDi 1.9C is vulnerable to Remote Command Execution. System-Snapshot.php improperly escapes shell metacharacters from a POST request. An attacker can exploit this by crafting an arbitrary payload (any system commands) that contains shell metacharacters via a POST request with a psw parameter. (This can also be exploited via CSRF.) **CVE ID : CVE-2020-14412**	N/A	A-NED-NEDI-070820/417
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-06-2020	4.3	NeDi 1.9C is vulnerable to XSS because of an incorrect implementation of sanitize() in inc/libmisc.php. This function attempts to escape the SCRIPT tag from user-controllable values, but can be easily bypassed, as demonstrated by an onerror attribute of an IMG element as a Devices-Config.php?sta= value. **CVE ID : CVE-2020-14413**	N/A	A-NED-NEDI-070820/418
Improper Neutralization of Special Elements	29-06-2020	9	NeDi 1.9C is vulnerable to Remote Command Execution. pwsec.php improperly escapes shell	N/A	A-NED-NEDI-070820/419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			metacharacters from a POST request. An attacker can exploit this by crafting an arbitrary payload (any system commands) that contains shell metacharacters via a POST request with a pw parameter. (This can also be exploited via CSRF.) **CVE ID : CVE-2020-14414**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-06-2020	4.3	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Other-Converter.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the txt GET parameter. **CVE ID : CVE-2020-15016**	N/A	A-NED-NEDI-070820/420
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	26-06-2020	4.3	NeDi 1.9C is vulnerable to reflected cross-site scripting. The Devices-Config.php file improperly validates user input. An attacker can exploit this vulnerability by crafting arbitrary JavaScript in the sta GET parameter. **CVE ID : CVE-2020-15017**	N/A	A-NED-NEDI-070820/421
neomutt					
neomutt					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	21-06-2020	4.3	Mutt before 1.14.4 and NeoMutt before 2020-06-19 have a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a	N/A	A-NEO-NEOM-070820/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			man-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-14954**		
Netflix					
conductor					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-06-2020	7.5	Netflix Titus uses Java Bean Validation (JSR 380) custom constraint validators. When building custom constraint violation error messages, different types of interpolation are supported, including Java EL expressions. If an attacker can inject arbitrary data in the error message template being passed to ConstraintValidatorContext.buildConstraintViolationWithTemplate() argument, they will be able to run arbitrary Java code. **CVE ID : CVE-2020-9296**	N/A	A-NET-COND-070820/423
neutrinolabs					
xrdp					
Stack-based Buffer Overflow	30-06-2020	4.6	The xrdp-sesman service before version 0.9.13.1 can be crashed by connecting over port 3350 and supplying a malicious payload. Once the xrdp-sesman process is dead, an unprivileged attacker on the server could then proceed to start their own imposter sesman service listening on port 3350. This will allow	https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-j9fv-6fwf-p3g4	A-NEU-XRDP-070820/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			them to capture any user credentials that are submitted to XRDP and approve or reject arbitrary login credentials. For xorgxrdp sessions in particular, this allows an unauthorized user to hijack an existing session. This is a buffer overflow attack, so there may be a risk of arbitrary code execution as well. **CVE ID : CVE-2020-4044**		
nexos_project					
nexos					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-06-2020	5	The Nexos theme through 1.7 for WordPress allows side-map/?search_order= SQL Injection. **CVE ID : CVE-2020-15363**	N/A	A-NEX-NEXO-070820/425
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-06-2020	4.3	The Nexos theme through 1.7 for WordPress allows top-map/?search_location= reflected XSS. **CVE ID : CVE-2020-15364**	N/A	A-NEX-NEXO-070820/426
nozominetworks					
guardian					
Improper Neutralization of Input During Web	30-06-2020	4.3	Nozomi Guardian before 19.0.4 allows attackers to achieve stored XSS (in the web front end) by leveraging	N/A	A-NOZ-GUAR-070820/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			the ability to create a custom field with a crafted field name. **CVE ID : CVE-2020-15307**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	30-06-2020	8.5	Nozomi Networks OS before 19.0.4 allows /#/network?tab=network_node_list.html CSV Injection. **CVE ID : CVE-2020-7049**	N/A	A-NOZ-GUAR-070820/428
nta					
e-tax_reception_system					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	30-06-2020	6.8	Chrome Extension for e-Tax Reception System Ver1.0.0.0 allows remote attackers to execute an arbitrary command via unspecified vectors. **CVE ID : CVE-2020-5601**	N/A	A-NTA-E-TA-070820/429
NTP					
ntp					
Improper Release of Memory Before Removing Last Reference	24-06-2020	4	ntpd in ntp 4.2.8 before 4.2.8p15 and 4.3.x before 4.3.101 allows remote attackers to cause a denial of service (memory consumption) by sending packets, because memory is not freed in situations where a CMAC key is used and associated with a CMAC algorithm in the ntp.keys file.	https://security.netapp.com/advisory/ntap-20200702-0002/	A-NTP-NTP-070820/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15025		
nukeviet					
nukeviet					
Cross-Site Request Forgery (CSRF)	23-06-2020	6.8	clearsystem.php in NukeViet 4.4 allows CSRF with resultant HTML injection via the deltype parameter to the admin/index.php?nv=webtools&op=clearsystem URI. **CVE ID : CVE-2020-13155**	N/A	A-NUK-NUKE-070820/431
Cross-Site Request Forgery (CSRF)	23-06-2020	4.3	modules\users\admin\add_user.php in NukeViet 4.4 allows CSRF to add a user account via the admin/index.php?nv=users&op=user_add URI. **CVE ID : CVE-2020-13156**	N/A	A-NUK-NUKE-070820/432
Cross-Site Request Forgery (CSRF)	23-06-2020	4.3	modules\users\admin\edit.php in NukeViet 4.4 allows CSRF to change a user's password via an admin/index.php?nv=users&op=edit&userid= URI. The old password is not needed. **CVE ID : CVE-2020-13157**	N/A	A-NUK-NUKE-070820/433
Nvidia					
geforce_experience					
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/50	A-NVI-GEFO-070820/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5964	38	
virtual_gpu_manager					
Improper Restriction of Operations within the Bounds of a Memory Buffer	30-06-2020	4.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which the software does not restrict or incorrectly restricts operations within the boundaries of a resource that is accessed by using an index or pointer, such as memory or files, which may lead to code execution, denial of service, escalation of privileges, or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3). **CVE ID : CVE-2020-5968**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	A-NVI-VIRT-070820/435
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	30-06-2020	3.3	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which it validates a shared resource before using it, creating a race condition which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3). **CVE ID : CVE-2020-5969**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	A-NVI-VIRT-070820/436
Improper Input Validation	30-06-2020	3.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which an input data size is not validated, which may lead to tampering or denial of	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	A-NVI-VIRT-070820/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3). **CVE ID : CVE-2020-5970**		
Out-of-bounds Read	30-06-2020	4.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which the software reads from a buffer by using buffer access mechanisms such as indexes or pointers that reference memory locations after the targeted buffer, which may lead to code execution, denial of service, escalation of privileges, or information disclosure. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3). **CVE ID : CVE-2020-5971**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	A-NVI-VIRT-070820/438
Release of Invalid Pointer or Reference	30-06-2020	3.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which local pointer variables are not initialized and may be freed later, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3). **CVE ID : CVE-2020-5972**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	A-NVI-VIRT-070820/439
virtual_gpu					
Improper Input Validation	30-06-2020	2.1	NVIDIA Virtual GPU Manager and the guest drivers contain a vulnerability in vGPU plugin, in which there is the	https://nvidia.custhelp.com/app/answers/det	A-NVI-VIRT-070820/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential to execute privileged operations, which may lead to denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3). **CVE ID : CVE-2020-5973**	ail/a_id/5031	
oauth2_proxy_project					
oauth2_proxy					
URL Redirection to Untrusted Site ('Open Redirect')	29-06-2020	5.8	In OAuth2 Proxy from version 5.1.1 and less than version 6.0.0, users can provide a redirect address for the proxy to send the authenticated user to at the end of the authentication flow. This is expected to be the original URL that the user was trying to access. This redirect URL is checked within the proxy and validated before redirecting the user to prevent malicious actors providing redirects to potentially harmful sites. This has been fixed in version 6.0.0. **CVE ID : CVE-2020-4037**	https://github.com/oauth2-proxy/oauth2-proxy/security/advisories/GHSA-5m6c-jp6f-2vcv	A-OAU-OAUT-070820/441
obdev					
little_snitch					
Improper Link Resolution Before File Access ('Link Following')	30-06-2020	9	Little Snitch version 4.5.1 and older changed ownership of a directory path controlled by the user. This allowed the user to escalate to root by linking the path to a directory containing code executed by	N/A	A-OBD-LITT-070820/442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			root. **CVE ID : CVE-2020-13095**		
octopus					
octopus_deploy					
Insufficiently Protected Credentials	19-06-2020	4	In Octopus Deploy 2018.8.0 through 2019.x before 2019.12.2, an authenticated user with could trigger a deployment that leaks the Helm Chart repository password. **CVE ID : CVE-2020-14470**	N/A	A-OCT-OCTO-070820/443
oneidentity					
syslog-ng					
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise	https://bugzilla.suse.com/show_bug.cgi?id=1169385	A-ONE-SYSL-070820/444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1. **CVE ID : CVE-2020-8019**		
Openbsd					
openssh					
Information Exposure	29-06-2020	4.3	The client side in OpenSSH 5.7 through 8.3 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). **CVE ID : CVE-2020-14145**	https://security.netapp.com/advisory/ntap-20200709-0004/	A-OPE-OPEN-070820/445
Openexr					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
openexr					
NULL Pointer Dereference	26-06-2020	2.1	An issue was discovered in OpenEXR before 2.5.2. An invalid tiled input file could cause invalid memory access in TiledInputFile::TiledInputFile() in IlmImf/ImfTiledInputFile.cpp, as demonstrated by a NULL pointer dereference. **CVE ID : CVE-2020-15304**	N/A	A-OPE-OPEN-070820/446
Use After Free	26-06-2020	2.1	An issue was discovered in OpenEXR before 2.5.2. Invalid input could cause a use-after-free in DeepScanLineInputFile::DeepScanLineInputFile() in IlmImf/ImfDeepScanLineInputFile.cpp. **CVE ID : CVE-2020-15305**	N/A	A-OPE-OPEN-070820/447
Out-of-bounds Write	26-06-2020	2.1	An issue was discovered in OpenEXR before v2.5.2. Invalid chunkCount attributes could cause a heap buffer overflow in getChunkOffsetTableSize() in IlmImf/ImfMisc.cpp. **CVE ID : CVE-2020-15306**	N/A	A-OPE-OPEN-070820/448
openfind					
mailaudit					
Improper Neutralization of Special Elements in Output Used by a Downstream	23-06-2020	7.5	Openfind MailGates contains a Command Injection flaw, when receiving email with specific strings, malicious code in the mail attachment will be triggered and gain unauthorized access to	https://www.twcert.org.tw/tw/cp-132-3688-271ea-1.html	A-OPE-MAIL-070820/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			system files. **CVE ID : CVE-2020-12782**		
mailgates					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-06-2020	7.5	Openfind MailGates contains a Command Injection flaw, when receiving email with specific strings, malicious code in the mail attachment will be triggered and gain unauthorized access to system files. **CVE ID : CVE-2020-12782**	https://www.twcert.org.tw/tw/cp-132-3688-271ea-1.html	A-OPE-MAIL-070820/450
openmicroscopy					
omero.web					
Information Exposure	17-06-2020	3.5	OMERO.web before 5.6.3 optionally allows sensitive data elements (e.g., a session key) to be passed as URL query parameters. If an attacker tricks a user into clicking a malicious link in OMERO.web, the information in the query parameters may be exposed in the Referer header seen by the target. Information in the URL path such as object IDs may also be exposed. **CVE ID : CVE-2020-7932**	https://www.openmicroscopy.org/security/advisories/2019-SV4/	A-OPE-OMER-070820/451
omero					
Information Exposure	17-06-2020	5.5	In OMERO before 5.6.1, group owners can access members' data in other groups. **CVE ID : CVE-2020-6752**	https://www.openmicroscopy.org/security/advisories/2019-SV6/	A-OPE-OMER-070820/452
Opensuse					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
backports_sle					
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1	https://bugzilla.suse.com/show_bug.cgi?id=1169385	A-OPE-BACK-070820/453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1. **CVE ID : CVE-2020-8019**		
tumbleweed_kopano-spamd					
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of kopano-spamd of openSUSE Leap 15.1, openSUSE Tumbleweed allowed local attackers with the privileges of the kopano user to escalate to root. This issue affects: openSUSE Leap 15.1 kopano-spamd versions prior to 10.0.5-lp151.4.1. openSUSE Tumbleweed kopano-spamd versions prior to 10.0.5-1.1. **CVE ID : CVE-2020-8014**	https://bugzilla.suse.com/show_bug.cgi?id=1164131	A-OPE-TUMB-070820/454
Open-xchange					
open-xchange_appsuite					
Improper Restriction of XML External Entity Reference ('XXE')	16-06-2020	4	OX App Suite through 7.10.3 allows XXE attacks. **CVE ID : CVE-2020-8541**	N/A	A-OPE-OPEN-070820/455
Improper Neutralization of Input During Web	16-06-2020	3.5	OX App Suite through 7.10.3 allows XSS. **CVE ID : CVE-2020-8542**	N/A	A-OPE-OPEN-070820/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')					
Uncontrolled Resource Consumption	16-06-2020	5	OX App Suite through 7.10.3 has Improper Input Validation. **CVE ID : CVE-2020-8543**	N/A	A-OPE-OPEN-070820/457
Server-Side Request Forgery (SSRF)	16-06-2020	4	OX App Suite through 7.10.3 allows SSRF. **CVE ID : CVE-2020-8544**	N/A	A-OPE-OPEN-070820/458
Osisoft					
pi_web_api					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-06-2020	6	In OSIsoft PI Web API 2019 Patch 1 (1.12.0.6346) and all previous versions, the affected product is vulnerable to a cross-site scripting attack, which may allow an attacker to remotely execute arbitrary code. **CVE ID : CVE-2020-12021**	N/A	A-OSI-PI_W-070820/459
Paessler					
prtg_network_monitor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-06-2020	3.5	XSS exists in PRTG Network Monitor 20.1.56.1574 via crafted map properties. An attacker with Read/Write privileges can create a map, and then use the Map Designer Properties screen to insert JavaScript code. This can be exploited against any user with View Maps or Edit Maps access.	N/A	A-PAE-PRTG-070820/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14073		
Php-fusion					
php-fusion					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-06-2020	6.5	A SQL injection vulnerability in PHP-Fusion 9.03.50 affects the endpoint administration/comments.php via the ctype parameter, **CVE ID : CVE-2020-14960**	N/A	A-PHP-PHP--070820/461
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	PHP-Fusion 9.03.60 allows XSS via the administration/site_links.php Add Site Link field. **CVE ID : CVE-2020-15041**	N/A	A-PHP-PHP--070820/462
pi-hole					
pi-hole					
Improper Control of Generation of Code ('Code Injection')	23-06-2020	4.6	Pi-hole through 5.0 allows code injection in piholedhcp (the Static DHCP Leases section) by modifying Teleporter backup files and then restoring them. This occurs in settings.php. To exploit this, an attacker would request a backup of limited files via teleporter.php. These are placed into a .tar.gz archive. The attacker then modifies the host parameter in dnsmasq.d files, and then compresses and uploads these files again.	https://github.com/pi-hole/AdminLTE/commit/8f6e1365b6dec0ae1aa0b0b15b102c9133f347e5, https://github.com/pi-hole/AdminLTE/commit/c949516ee15fa6a9b0c8511cc4c4d6b0893f3e	A-PI--PI-H-070820/463

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14971	69, https://github.com/pi-hole/AdminLTE/pull/1443	
Playsms					
playsms					
Session Fixation	24-06-2020	6.4	playSMS through 1.4.3 is vulnerable to session fixation. **CVE ID : CVE-2020-15018**	N/A	A-PLA-PLAY-070820/464
pramod					
blogcms					
Cross-Site Request Forgery (CSRF)	24-06-2020	6.8	pramodmahato BlogCMS through 2019-12-31 has admin/changepass.php CSRF. **CVE ID : CVE-2020-15014**	N/A	A-PRA-BLOG-070820/465
prestosql					
presto					
Improper Privilege Management	30-06-2020	6.5	In Presto before version 337, authenticated users can bypass authorization checks by directly accessing internal APIs. This impacts Presto server installations with secure internal communication configured. This does not affect installations that have not configured secure internal communication, as these installations are inherently insecure. This only affects Presto server installations. This does NOT affect clients such as the CLI or JDBC	https://github.com/prestosql/presto/security/advisories/GHSA-f6pc-crhh-cp96	A-PRE-PRES-070820/466

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver. This vulnerability has been fixed in version 337. Additionally, this issue can be mitigated by blocking network access to internal APIs on the coordinator and workers. **CVE ID : CVE-2020-15087**		
Pulsesecure					
pulse_secure_installer_service					
Time-of-check Time-of-use (TOCTOU) Race Condition	16-06-2020	6.9	A time-of-check time-of-use vulnerability in PulseSecureService.exe in Pulse Secure Client versions prior to 9.1.6 down to 5.3 R70 for Windows (which runs as NT AUTHORITY/SYSTEM) allows unprivileged users to run a Microsoft Installer executable with elevated privileges. **CVE ID : CVE-2020-13162**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44503	A-PUL-PULS-070820/467
pulse_secure_desktop_client					
Time-of-check Time-of-use (TOCTOU) Race Condition	16-06-2020	6.9	A time-of-check time-of-use vulnerability in PulseSecureService.exe in Pulse Secure Client versions prior to 9.1.6 down to 5.3 R70 for Windows (which runs as NT AUTHORITY/SYSTEM) allows unprivileged users to run a Microsoft Installer executable with elevated privileges. **CVE ID : CVE-2020-13162**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44503	A-PUL-PULS-070820/468
Putty					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
putty					
Information Exposure	29-06-2020	4.3	PuTTY 0.68 through 0.73 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). **CVE ID : CVE-2020-14002**	https://security.netapp.com/advisory/ntap-20200717-0003/	A-PUT-PUTT-070820/469
Python					
pillow					
Out-of-bounds Read	25-06-2020	4.3	In libImaging/PcxDecode.c in Pillow before 7.1.0, an out-of-bounds read can occur when reading PCX files where state->shuffle is instructed to read beyond state->buffer. **CVE ID : CVE-2020-10378**	N/A	A-PYT-PILL-070820/470
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-06-2020	6.8	In Pillow before 7.1.0, there are two Buffer Overflows in libImaging/TiffDecode.c. **CVE ID : CVE-2020-10379**	N/A	A-PYT-PILL-070820/471
Out-of-bounds Read	25-06-2020	4.3	Pillow before 7.1.0 has multiple out-of-bounds reads in libImaging/FliDecode.c. **CVE ID : CVE-2020-10177**	N/A	A-PYT-PILL-070820/472
Out-of-bounds Read	25-06-2020	4.3	In libImaging/Jpeg2KDecode.c in Pillow before 7.1.0, there are multiple out-of-bounds	N/A	A-PYT-PILL-070820/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reads via a crafted JP2 file. **CVE ID : CVE-2020-10994**		
Out-of-bounds Read	25-06-2020	6.8	In libImaging/SgiRleDecode.c in Pillow through 7.0.0, a number of out-of-bounds reads exist in the parsing of SGI image files, a different issue than CVE-2020-5311. **CVE ID : CVE-2020-11538**	N/A	A-PYT-PILL-070820/474
python					
Uncontrolled Resource Consumption	18-06-2020	4.3	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. **CVE ID : CVE-2020-14422**	N/A	A-PYT-PYTH-070820/475
rack_project					
rack					
Improper Input Validation	19-06-2020	5	A reliance on cookies without validation/integrity check security vulnerability exists in rack < 2.2.3, rack < 2.1.4 that makes it is possible for an attacker to forge a secure or host-only cookie prefix. **CVE ID : CVE-2020-8184**	N/A	A-RAC-RACK-070820/476

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rakuten					
viber					
Unquoted Search Path or Element	22-06-2020	5	Viber for Windows up to 13.2.0.39 does not properly quote its custom URI handler. A malicious website could launch Viber with arbitrary parameters, forcing a victim to send an NTLM authentication request, and either relay the request or capture the hash for offline password cracking. NOTE: this issue exists because of an incomplete fix for CVE-2019-12569. **CVE ID : CVE-2020-14049**	N/A	A-RAK-VIBE-070820/477
Rapid7					
metasploit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2020	4.3	Cross-site Scripting (XSS) vulnerability in the 'host' field of a discovered scan asset in Rapid7 Metasploit Pro allows an attacker with a specially-crafted network service of a scan target to store an XSS sequence in the Metasploit Pro console, which will trigger when the operator views the record of that scanned host in the Metasploit Pro interface. This issue affects Rapid7 Metasploit Pro version 4.17.1-20200427 and prior versions, and is fixed in Metasploit Pro version 4.17.1-20200514. See also	https://help.rapid7.com/metasploit/release-notes/archive/2020/05/#20200514	A-RAP-META-070820/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2020-7355, which describes a similar issue, but involving the generated 'notes' field of a discovered scan asset. **CVE ID : CVE-2020-7354**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2020	4.3	Cross-site Scripting (XSS) vulnerability in the 'notes' field of a discovered scan asset in Rapid7 Metasploit Pro allows an attacker with a specially-crafted network service of a scan target store an XSS sequence in the Metasploit Pro console, which will trigger when the operator views the record of that scanned host in the Metasploit Pro interface. This issue affects Rapid7 Metasploit Pro version 4.17.1-20200427 and prior versions, and is fixed in Metasploit Pro version 4.17.1-20200514. See also CVE-2020-7354, which describes a similar issue, but involving the generated 'host' field of a discovered scan asset. **CVE ID : CVE-2020-7355**	https://help.rapid7.com/metasploit/release-notes/archive/2020/05/#20200514	A-RAP-META-070820/479
Redhat					
wildfly					
Deserialization of Untrusted Data	22-06-2020	6	A vulnerability was found in Wildfly in versions before 20.0.0.Final, where a remote deserialization attack is possible in the Enterprise Application Beans(EJB) due	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10740	A-RED-WILD-070820/480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to lack of validation/filtering capabilities in wildfly. **CVE ID : CVE-2020-10740**		
keycloak					
Improper Input Validation	22-06-2020	5.5	A vulnerability was found in Keycloak before 9.0.2, where every Authorization URL that points to an IDP server lacks proper input validation as it allows a wide range of characters. This flaw allows a malicious to craft deep links that introduce further attack scenarios on affected clients. **CVE ID : CVE-2020-1727**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1727	A-RED-KEYC-070820/481
openstack					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-06-2020	4.3	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway). The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. Ceph versions 3.x and 4.x are vulnerable to this issue. **CVE ID : CVE-2020-10753**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10753	A-RED-OPEN-070820/482
ansible_tower					
Incorrect Default Permissions	18-06-2020	2.1	An exposure of sensitive information flaw was found in Ansible Tower before version 3.7.1. sensitive information such as Splunk	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-	A-RED-ANSI-070820/483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tokens could be readable in the rsyslog configuration file, which has set the wrong world-readable permissions. The highest threat from this vulnerability is to confidentiality. **CVE ID : CVE-2020-10782**	10782	
ceph_storage					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-06-2020	4.3	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway). The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. Ceph versions 3.x and 4.x are vulnerable to this issue. **CVE ID : CVE-2020-10753**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10753	A-RED-CEPH-070820/484
requarks					
wiki.js					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-06-2020	4.3	In Wiki.js before 2.4.107, there is a stored cross-site scripting through template injection. This vulnerability exists due to an insecure validation mechanism intended to insert v-pre tags into rendered HTML elements which contain curly-braces. By creating a crafted wiki page, a malicious Wiki.js user may stage a stored cross-site	https://github.com/Requarks/wiki/security/advisories/GHSA-9jgg-4xj2-vjjj	A-REQ-WIKI-070820/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scripting attack. This allows the attacker to execute malicious JavaScript when the page is viewed by other users. This has been patched in 2.4.107. **CVE ID : CVE-2020-4052**		
Rockwellautomation					
factorytalk_services_platform					
Improper Input Validation	23-06-2020	5.8	In Rockwell Automation FactoryTalk Services Platform, all versions, the redundancy host service (RdcyHost.exe) does not validate supplied identifiers, which could allow an unauthenticated, adjacent attacker to execute remote COM objects with elevated privileges. **CVE ID : CVE-2020-12033**	N/A	A-ROC-FACT-070820/486
rtslib-fb_project					
rtslib-fb					
Incorrect Default Permissions	19-06-2020	7.5	Open-iSCSI rtslib-fb through 2.1.72 has weak permissions for /etc/target/saveconfig.json because shutil.copyfile (instead of shutil.copy) is used, and thus permissions are not preserved. **CVE ID : CVE-2020-14019**	N/A	A-RTS-RTSL-070820/487
Rubyonrails					
rails					
Unrestricted Upload of File with	19-06-2020	5	A client side enforcement of server side security vulnerability exists in rails <	N/A	A-RUB-RAIL-070820/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			5.2.4.2 and rails < 6.0.3.1 ActiveStorage's S3 adapter that allows the Content-Length of a direct file upload to be modified by an end user bypassing upload limits. **CVE ID : CVE-2020-8162**		
Deserialization of Untrusted Data	19-06-2020	5	A deserialization of untrusted data vulnerability exists in rails < 5.2.4.3, rails < 6.0.3.1 which can allow an attacker to supply information can be inadvertently leaked fromStrong Parameters. **CVE ID : CVE-2020-8164**	N/A	A-RUB-RAIL-070820/489
Deserialization of Untrusted Data	19-06-2020	7.5	A deserialization of untrusted data vulnernerability exists in rails < 5.2.4.3, rails < 6.0.3.1 that can allow an attacker to unmarshal user-provided objects in MemCacheStore and RedisCacheStore potentially resulting in an RCE. **CVE ID : CVE-2020-8165**	https://weblog.rubyonrails.org/2020/5/18/Rails-5-2-4-3-and-6-0-3-1-have-been-released/	A-RUB-RAIL-070820/490
Cross-Site Request Forgery (CSRF)	19-06-2020	4.3	A CSRF vulnerability exists in rails <= 6.0.3 rails-ujs module that could allow attackers to send CSRF tokens to wrong domains. **CVE ID : CVE-2020-8167**	N/A	A-RUB-RAIL-070820/491
sanitize_project					
sanitize					
Improper Neutralization of Input	16-06-2020	6.8	In Sanitize (RubyGem sanitize) greater than or equal to 3.0.0 and less than	https://github.com/rgrove/sanitiz	A-SAN-SANI-070820/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			5.2.1, there is a cross-site scripting vulnerability. When HTML is sanitized using Sanitize's "relaxed" config, or a custom config that allows certain elements, some content in a math or svg element may not be sanitized correctly even if math and svg are not in the allowlist. You are likely to be vulnerable to this issue if you use Sanitize's relaxed config or a custom config that allows one or more of the following HTML elements: iframe, math, noembed, noframes, noscript, plaintext, script, style, svg, xmp. Using carefully crafted input, an attacker may be able to sneak arbitrary HTML through Sanitize, potentially resulting in XSS (cross-site scripting) or other undesired behavior when that HTML is rendered in a browser. This has been fixed in 5.2.1. **CVE ID : CVE-2020-4054**	e/security/advisories/GHSA-p4x4-rw2p-8j8m	
SAS					
go_rpm_utils					
Improper Input Validation	24-06-2020	5	In package github.com/sassoftware/go-rpmutils/cpio before version 0.1.0, the CPIO extraction functionality doesn't sanitize the paths of the archived files for leading and non-leading ".." which leads in file	https://github.com/sassoftware/go-rpmutils/commit/a64058cf21b8aada501bba9	A-SAS-GO_R-070820/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			extraction outside of the current directory. Note: the fixing commit was applied to all affected versions which were re-released. **CVE ID : CVE-2020-7667**	23c9aab66fb6febf0, https://snyk.io/vuln/SNYK-GOLANG-GITHUBCOMSASSOFTWAREGORPMUTILSCPIO-570427	
Schneider-electric					
ecostruxure_operator_terminal_expert					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	6.8	A CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause malicious code execution when opening the project file. **CVE ID : CVE-2020-7493**	N/A	A-SCH-ECOS-070820/494
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-06-2020	6.8	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause malicious code execution when opening the project file. **CVE ID : CVE-2020-7494**	N/A	A-SCH-ECOS-070820/495

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-06-2020	4.3	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability during zip file extraction exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD) which could cause unauthorized write access outside of expected path folder when opening the project file. **CVE ID : CVE-2020-7495**	N/A	A-SCH-ECOS-070820/496
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-06-2020	7.5	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD)which could cause arbitrary application execution when the computer starts. **CVE ID : CVE-2020-7497**	N/A	A-SCH-ECOS-070820/497
gp-pro_ex_firmware					
Weak Password Requirements	16-06-2020	4.3	A CWE-521: Weak Password Requirements vulnerability exists in the GP-Pro EX V1.00 to V4.09.100 which could cause the discovery of the password when the user is entering the password because it is not masqueraded. **CVE ID : CVE-2020-7492**	N/A	A-SCH-GP-P-070820/498

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
se					
ecostruxure_operator_terminal_expert					
Argument Injection or Modification	16-06-2020	6.8	A CWE-88: Argument Injection or Modification vulnerability exists in EcoStruxure Operator Terminal Expert 3.1 Service Pack 1 and prior (formerly known as Vijeo XD)which could cause unauthorized write access when opening the project file. **CVE ID : CVE-2020-7496**	N/A	A-SE-ECOS-070820/499
vijeo_designer					
Use of Hard-coded Credentials	16-06-2020	6.5	A CWE-798: Use of Hard-coded Credentials vulnerability exists in Vijeo Designer Basic (V1.1 HotFix 16 and prior) and Vijeo Designer (V6.2 SP9 and prior) which could cause unauthorized read and write when downloading and uploading project or firmware into Vijeo Designer Basic and Vijeo Designer. **CVE ID : CVE-2020-7501**	N/A	A-SE-VIJE-070820/500
os_loader					
Use of Hard-coded Credentials	16-06-2020	7.5	A CWE-798: Use of Hard-coded Credentials vulnerability exists in the Unity Loader and OS Loader Software (all versions). The fixed credentials are used to simplify file transfer. Today the use of fixed credentials is considered a vulnerability, which could cause unauthorized access to the	N/A	A-SE-OS_L-070820/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file transfer service provided by the Modicon PLCs. This could result in various unintended results. **CVE ID : CVE-2020-7498**		
unity_loader					
Use of Hard-coded Credentials	16-06-2020	7.5	A CWE-798: Use of Hard-coded Credentials vulnerability exists in the Unity Loader and OS Loader Software (all versions). The fixed credentials are used to simplify file transfer. Today the use of fixed credentials is considered a vulnerability, which could cause unauthorized access to the file transfer service provided by the Modicon PLCs. This could result in various unintended results. **CVE ID : CVE-2020-7498**	N/A	A-SE-UNIT-070820/502
secureauth					
secureauth_identity_provider					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	25-06-2020	3.5	SecureAuth.aspx in SecureAuth IdP 9.3.0 suffers from a client-side template injection that allows for script execution, in the same manner as XSS. **CVE ID : CVE-2020-9437**	N/A	A-SEC-SECU-070820/503
seedprod					
coming_soon_page\,_under_construction_\&_maintenance_mode					
Improper Neutralization of Input During Web	24-06-2020	3.5	The SeedProd coming-soon plugin before 5.1.1 for WordPress allows XSS.	N/A	A-SEE-COMI-070820/504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2020-15038**		
semtech					
loramac-node					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	23-06-2020	6.5	In LoRaMac-node before 4.4.4, a reception buffer overflow can happen due to the received buffer size not being checked. This has been fixed in 4.4.4. **CVE ID : CVE-2020-11068**	https://github.com/Lora-net/LoRaMac-node/security/advisories/GHSA-559p-6xgm-fpv9	A-SEM-LORA-070820/505
lora_basics_station					
Use After Free	22-06-2020	4	In LoRa Basics Station before 2.0.4, there is a Use After Free vulnerability that leads to memory corruption. This bug is triggered on 32-bit machines when the CUPS server responds with a message (https://doc.sm.tc/station/cupsproto.html#http-post-response) where the signature length is larger than 2 GByte (never happens in practice), or the response is crafted specifically to trigger this issue (i.e. the length signature field indicates a value larger than (2**31)-1 although the signature actually does not contain that much data). In such a scenario, on 32 bit machines, Basic Station	https://github.com/lorabasics/basicstation/security/advisories/GHSA-v9ph-r496-4m2j	A-SEM-LORA-070820/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would execute a code path, where a piece of memory is accessed after it has been freed, causing the process to crash and restarted again. The CUPS transaction is typically mutually authenticated over TLS. Therefore, in order to trigger this vulnerability, the attacker would have to gain access to the CUPS server first. If the user chose to operate without authentication over TLS but yet is concerned about this vulnerability, one possible workaround is to enable TLS authentication. This has been fixed in 2.0.4. **CVE ID : CVE-2020-4060**		
Solarwinds					
orion_web_performance_monitor					
N/A	24-06-2020	9	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows remote attackers to execute arbitrary code via a defined event. **CVE ID : CVE-2020-14005**	N/A	A-SOL-ORIO-070820/507
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows XSS via a Responsible Team. **CVE ID : CVE-2020-14006**	N/A	A-SOL-ORIO-070820/508

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows XSS via a name of an alert definition. **CVE ID : CVE-2020-14007**	N/A	A-SOL-ORIO-070820/509
orion_network_performance_monitor					
N/A	24-06-2020	9	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows remote attackers to execute arbitrary code via a defined event. **CVE ID : CVE-2020-14005**	N/A	A-SOL-ORIO-070820/510
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows XSS via a Responsible Team. **CVE ID : CVE-2020-14006**	N/A	A-SOL-ORIO-070820/511
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-06-2020	3.5	Solarwinds Orion (with Web Console WPM 2019.4.1, and Orion Platform HF4 or NPM HF2 2019.4) allows XSS via a name of an alert definition. **CVE ID : CVE-2020-14007**	N/A	A-SOL-ORIO-070820/512
Sophos					
sophos_secure_email					
Improper Certificate Validation	22-06-2020	4.3	The Sophos Secure Email application through 3.9.4 for Android has Missing SSL	N/A	A-SOP-SOPH-070820/513

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Certificate Validation. **CVE ID : CVE-2020-14980**		
sourcecodester					
pisay_online_e-learning_system					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22-06-2020	7.5	Multiple SQL injection vulnerabilities in Sourcecodester Pisay Online E-Learning System 1.0 allow remote unauthenticated attackers to bypass authentication and achieve Remote Code Execution (RCE) via the user_email, user_pass, and id parameters on the admin login-portal and the edit-lessons webpages. **CVE ID : CVE-2020-14972**	N/A	A-SOU-PISA-070820/514
Sqlite					
sqlite					
Out-of-bounds Write	27-06-2020	2.1	In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation. **CVE ID : CVE-2020-15358**	https://security.netapp.com/advisory/ntap-20200709-0001/	A-SQL-SQLI-070820/515
Squid-cache					
squid					
NULL Pointer Dereference	30-06-2020	5	An issue was discovered in Squid before 4.12 and 5.x before 5.0.3. Due to use of a potentially dangerous function, Squid and the default certificate validation	http://www.squid-cache.org/Advisories/SQUID-2020_6.txt	A-SQU-SQUI-070820/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			helper are vulnerable to a Denial of Service when opening a TLS connection to an attacker-controlled server for HTTPS. This occurs because unrecognized error values are mapped to NULL, but later code expects that each error value is mapped to a valid error string. **CVE ID : CVE-2020-14058**		
Improper Synchronization	30-06-2020	4	An issue was discovered in Squid 5.x before 5.0.3. Due to an Incorrect Synchronization, a Denial of Service can occur when processing objects in an SMP cache because of an Ipc::Mem::PageStack::pop ABA problem during access to the memory page/slot management list. **CVE ID : CVE-2020-14059**	http://www.squid-cache.org/Advisories/SQUID-2020_5.txt	A-SQU-SQUI-070820/517
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	30-06-2020	6.5	An issue was discovered in http/ContentLengthInterpreter.cc in Squid before 4.12 and 5.x before 5.0.3. A Request Smuggling and Poisoning attack can succeed against the HTTP cache. The client sends an HTTP request with a Content-Length header containing "+\ "-" or an uncommon shell whitespace character prefix to the length field-value. **CVE ID : CVE-2020-15049**	https://github.com/squid-cache/squid/security/advisories/GHSA-qf3v-rc95-96j5	A-SQU-SQUI-070820/518

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Squirrelmail					
squirrelmail					
Deserialization of Untrusted Data	20-06-2020	7.5	compose.php in SquirrelMail 1.4.22 calls unserialize for the $mailtodata value, which originates from an HTTP GET request. This is related to mailto.php. **CVE ID : CVE-2020-14932**	N/A	A-SQU-SQUI-070820/519
Deserialization of Untrusted Data	20-06-2020	7.5	compose.php in SquirrelMail 1.4.22 calls unserialize for the $attachments value, which originates from an HTTP POST request. **CVE ID : CVE-2020-14933**	N/A	A-SQU-SQUI-070820/520
stash_cms_project					
stash_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-06-2020	7.5	Stash 1.0.3 allows SQL Injection via the downloadmp3.php download parameter. **CVE ID : CVE-2020-15311**	N/A	A-STA-STAS-070820/521
strapi					
strapi					
Improper Input Validation	19-06-2020	4	Strapi before 3.0.2 could allow a remote authenticated attacker to bypass security restrictions because templates are stored in a global variable without any sanitation. By sending a specially crafted request, an attacker could exploit this vulnerability to	https://github.com/strapi/strapi/pull/6599, https://github.com/strapi/strapi/releases/tag/v3.0.2	A-STR-STRA-070820/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			update the email template for both password reset and account confirmation emails. **CVE ID : CVE-2020-13961**		
Suse					
linux_enterprise_debuginfo					
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior	https://bugzilla.suse.com/show_bug.cgi?id=1169385	A-SUS-LINU-070820/523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1. **CVE ID : CVE-2020-8019**		
linux_enterprise_module_for_legacy					
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1.	https://bugzilla.suse.com/show_bug.cgi?id=1169385	A-SUS-LINU-070820/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1. **CVE ID : CVE-2020-8019**		
linux_enterprise_point_of_sale					
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise	https://bugzilla.suse.com/show_bug.cgi?id=1169385	A-SUS-LINU-070820/525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1. **CVE ID : CVE-2020-8019**		
enterprise_storage					
Incorrect Default Permissions	29-06-2020	7.2	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5,	https://bugzilla.suse.com/show_bug.cgi?id=11	A-SUS-ENTE-070820/526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux	72405	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1. **CVE ID : CVE-2020-8022**		
openstack_cloud					
Incorrect Default Permissions	29-06-2020	7.2	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS,	https://bugzilla.suse.com/show_bug.cgi?id=1172405	A-SUS-OPEN-070820/527

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1. **CVE ID : CVE-2020-8022**		
openstack_cloud_crowbar					
Incorrect Default Permissions	29-06-2020	7.2	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This	https://bugzilla.suse.com/show_bug.cgi?id=1172405	A-SUS-OPEN-070820/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0.53-29.32.1. **CVE ID : CVE-2020-8022**		
Tendenci					
tendenci					
Deserialization of Untrusted Data	21-06-2020	7.5	Tendenci 12.0.10 allows unrestricted deserialization in apps\helpdesk\views\staff.py. **CVE ID : CVE-2020-14942**	N/A	A-TEN-TEND-070820/529
thingssdk					
wifiscanner					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	29-06-2020	7.5	wifiscanner.js in thingsSDK WiFi Scanner 1.0.1 allows Code Injection because it can be used with options to overwrite the default executable/binary path and its arguments. An attacker can abuse this functionality to execute arbitrary code. **CVE ID : CVE-2020-15362**	N/A	A-THI-WIFI-070820/530
Tibco					
managed_file_transfer_command_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-06-2020	9.3	The MFT Browser file transfer client and MFT Browser admin client components of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contain a vulnerability that theoretically allows an attacker to craft an URL that will execute arbitrary	http://www.tibco.com/services/support/advisories	A-TIB-MANA-070820/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands on the affected system. If the attacker convinces an authenticated user with a currently active session to enter or click on the URL the commands will be executed on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions 8.2.1 and below. **CVE ID : CVE-2020-9413**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-06-2020	9	The MFT admin service component of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contains a vulnerability that theoretically allows an authenticated user with specific permissions to obtain the session identifier of another user. The session identifier when replayed could provide administrative rights or file transfer permissions to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions	http://www.tibco.com/services/support/advisories	A-TIB-MANA-070820/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.2.1 and below. **CVE ID : CVE-2020-9414**		
managed_file_transfer_internet_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-06-2020	9.3	The MFT Browser file transfer client and MFT Browser admin client components of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contain a vulnerability that theoretically allows an attacker to craft an URL that will execute arbitrary commands on the affected system. If the attacker convinces an authenticated user with a currently active session to enter or click on the URL the commands will be executed on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions 8.2.1 and below. **CVE ID : CVE-2020-9413**	http://www.tibco.com/services/support/advisories	A-TIB-MANA-070820/533
Improper Neutralization of Input During Web Page Generation ('Cross-site	30-06-2020	9	The MFT admin service component of TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center and TIBCO Managed File Transfer Internet Server contains a vulnerability that	http://www.tibco.com/services/support/advisories	A-TIB-MANA-070820/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			theoretically allows an authenticated user with specific permissions to obtain the session identifier of another user. The session identifier when replayed could provide administrative rights or file transfer permissions to the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Managed File Transfer Command Center: versions 8.2.1 and below and TIBCO Managed File Transfer Internet Server: versions 8.2.1 and below. **CVE ID : CVE-2020-9414**		
treck					
tcp\/ip					
Improper Input Validation	17-06-2020	9.3	The Treck TCP/IP stack before 6.0.1.66 allows Remote Code Execution, related to IPv4 tunneling. **CVE ID : CVE-2020-11896**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://cert-portal.siemens.com/productcert/pdf/ssa-631949.pdf, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-06-2020	10	The Treck TCP/IP stack before 5.0.1.35 has an Out-of-Bounds Write via multiple malformed IPv6 packets. **CVE ID : CVE-2020-11897**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt	A-TRE-TCP\-070820/536
Information Exposure	17-06-2020	6.4	The Treck TCP/IP stack before 6.0.1.66 improperly handles an IPv4/ICMPv4 Length Parameter Inconsistency, which might allow remote attackers to trigger an information leak. **CVE ID : CVE-2020-11898**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/537
Out-of-bounds Read	17-06-2020	4.8	The Treck TCP/IP stack before 6.0.1.66 has an IPv6 Out-of-bounds Read. **CVE ID : CVE-2020-11899**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/, https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-	A-TRE-TCP\-070820/538

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				00295.html	
Double Free	17-06-2020	6.4	The Treck TCP/IP stack before 6.0.1.41 has an IPv4 tunneling Double Free. **CVE ID : CVE-2020-11900**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/, https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html	A-TRE-TCP\-070820/539
Improper Input Validation	17-06-2020	9.3	The Treck TCP/IP stack before 6.0.1.66 allows Remote Code execution via a single invalid DNS response. **CVE ID : CVE-2020-11901**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt	A-TRE-TCP\-070820/540
Out-of-bounds Read	17-06-2020	7.5	The Treck TCP/IP stack before 6.0.1.66 has an IPv6OverIPv4 tunneling Out-of-bounds Read. **CVE ID : CVE-2020-11902**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advi	A-TRE-TCP\-070820/541

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				sory/ntap-20200625-0006/	
Out-of-bounds Read	17-06-2020	3.3	The Treck TCP/IP stack before 6.0.1.28 has a DHCP Out-of-bounds Read. **CVE ID : CVE-2020-11903**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/542
Out-of-bounds Write	17-06-2020	7.5	The Treck TCP/IP stack before 6.0.1.66 has an Integer Overflow during Memory Allocation that causes an Out-of-Bounds Write. **CVE ID : CVE-2020-11904**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/543
Out-of-bounds Read	17-06-2020	3.3	The Treck TCP/IP stack before 6.0.1.66 has a DHCPv6 Out-of-bounds Read. **CVE ID : CVE-2020-11905**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-	A-TRE-TCP\-070820/544

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				20200625-0006/, https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00295.html	
Integer Underflow (Wrap or Wraparound)	17-06-2020	5.8	The Treck TCP/IP stack before 6.0.1.66 has an Ethernet Link Layer Integer Underflow. **CVE ID : CVE-2020-11906**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/545
N/A	17-06-2020	5.8	The Treck TCP/IP stack before 6.0.1.66 improperly handles a Length Parameter Inconsistency in TCP. **CVE ID : CVE-2020-11907**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/546
N/A	17-06-2020	3.3	The Treck TCP/IP stack before 4.7.1.27 mishandles '\0' termination in DHCP.	http://www.arubanetworks.com/	A-TRE-TCP\-070820/547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11908	assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	
Integer Underflow (Wrap or Wraparound)	17-06-2020	5	The Treck TCP/IP stack before 6.0.1.66 has an IPv4 Integer Underflow. **CVE ID : CVE-2020-11909**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/548
Out-of-bounds Read	17-06-2020	5	The Treck TCP/IP stack before 6.0.1.66 has an ICMPv4 Out-of-bounds Read. **CVE ID : CVE-2020-11910**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/549
Missing Authorization	17-06-2020	5	The Treck TCP/IP stack before 6.0.1.66 has Improper ICMPv4 Access Control. **CVE ID : CVE-2020-11911**	http://www.arubanetworks.com/assets/alert	A-TRE-TCP\-070820/550

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	
Out-of-bounds Read	17-06-2020	3.3	The Treck TCP/IP stack before 6.0.1.66 has a TCP Out-of-bounds Read. **CVE ID : CVE-2020-11912**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/551
Out-of-bounds Read	17-06-2020	5	The Treck TCP/IP stack before 6.0.1.66 has an IPv6 Out-of-bounds Read. **CVE ID : CVE-2020-11913**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	A-TRE-TCP\-070820/552
Out-of-bounds Read	17-06-2020	3.3	The Treck TCP/IP stack before 6.0.1.66 has an ARP Out-of-bounds Read. **CVE ID : CVE-2020-11914**	http://www.arubanetworks.com/assets/alert/ARUBA-	A-TRE-TCP\-070820/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				PSA-2020-006.txt, https://security.netapp.com/advisory/ntap-20200625-0006/	
trojita_project					
trojita					
Improper Certificate Validation	25-06-2020	4.3	MSA/SMTP.cpp in Trojita before 0.8 ignores certificate-verification errors, which allows man-in-the-middle attackers to spoof SMTP servers. **CVE ID : CVE-2020-15047**	N/A	A-TRO-TROJ-070820/554
turnkeylinux					
support_incident_tracker					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	26-06-2020	6.5	Support Incident Tracker (aka SiT! or SiTracker) 3.67 p2 allows post-authentication SQL injection via the site_edit.php typeid or site parameter, the search_incidents_advanced.php search_title parameter, or the report_qbe.php criteriafield parameter. **CVE ID : CVE-2020-15308**	N/A	A-TUR-SUPP-070820/555
uclouvain					
openjpeg					
Use After Free	29-06-2020	5.8	jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be triggered if there is a mix of valid and invalid files in a directory operated on by the	N/A	A-UCL-OPEN-070820/556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			decompressor. Triggering a double-free may also be possible. This is related to calling opj_image_destroy twice. **CVE ID : CVE-2020-15389**		
Unisys					
stealth					
Incorrect Authorization	22-06-2020	7.5	In Unisys Stealth 3.4.x, 4.x and 5.x before 5.0.026, if certificate-based authorization is used without HTTPS, an endpoint could be authorized without a private key. **CVE ID : CVE-2020-12053**	https://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=54	A-UNI-STEA-070820/557
verint					
workforce_optimization					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-06-2020	3.5	Verint Workforce Optimization (WFO) 15.2 allows HTML injection via the "send email" feature. **CVE ID : CVE-2020-13480**	N/A	A-VER-WORK-070820/558
victorcms_project					
victorcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	4.3	Victor CMS 1.0 has Persistent XSS in admin/users.php?source=add_user via the user_name, user_firstname, or user_lastname parameter. **CVE ID : CVE-2020-13427**	N/A	A-VIC-VICT-070820/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vipre					
password_vault					
Improper Certificate Validation	22-06-2020	4.3	The ThreatTrack VIPRE Password Vault app through 1.100.1090 for iOS has Missing SSL Certificate Validation. **CVE ID : CVE-2020-14981**	N/A	A-VIP-PASS-070820/560
Vmware					
tools					
Improper Input Validation	19-06-2020	2.1	VMware Tools for macOS (11.x.x and prior before 11.1.1) contains a denial-of-service vulnerability in the Host-Guest File System (HGFS) implementation. Successful exploitation of this issue may allow attackers with non-admin privileges on guest macOS virtual machines to create a denial-of-service condition on their own VMs. **CVE ID : CVE-2020-3972**	N/A	A-VMW-TOOL-070820/561
workstation					
Use After Free	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a use-after-free vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/562

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. **CVE ID : CVE-2020-3962**		
Use After Free	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a use-after-free vulnerability in PVNVRAM. A malicious actor with local access to a virtual machine may be able to read privileged information contained in physical memory. **CVE ID : CVE-2020-3963**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/563
Information Exposure	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the EHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in the hypervisor's memory. Additional conditions beyond the attacker's control need to be present	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/564

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation to be possible. **CVE ID : CVE-2020-3964**		
Information Exposure	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the XHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine. **CVE ID : CVE-2020-3965**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/565
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	3.7	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a heap-overflow due to a race condition issue in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			present for exploitation to be possible. **CVE ID : CVE-2020-3966**		
Out-of-bounds Write	25-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a heap-overflow vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3967**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/567
Out-of-bounds Write	25-06-2020	4.6	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds write vulnerability in the USB 3.0 controller (xHCI). A malicious actor with local administrative privileges on a virtual machine may be able to exploit this issue to	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash the virtual machine's vmx process leading to a denial of service condition or execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3968**		
Off-by-one Error	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an off-by-one heap-overflow vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3969**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/569
Out-of-bounds Read	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x	https://www.vmware.com/security/advisories/VMSA-2020-	A-VMW-WORK-070820/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds read vulnerability in the Shader functionality. A malicious actor with non-administrative local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to crash the virtual machine's vmx process leading to a partial denial of service condition. **CVE ID : CVE-2020-3970**	0015.html	
Out-of-bounds Write	25-06-2020	2.1	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201907101-SG), Workstation (15.x before 15.0.2), and Fusion (11.x before 11.0.2) contain a heap overflow vulnerability in the vmxnet3 virtual network adapter. A malicious actor with local access to a virtual machine with a vmxnet3 network adapter present may be able to read privileged information contained in physical memory. **CVE ID : CVE-2020-3971**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-WORK-070820/571
fusion					
Use After Free	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x	https://www.vmware.com/security/advisories/VMSA-2020-	A-VMW-FUSI-070820/572

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 15.5.5), and Fusion (11.x before 11.5.5) contain a use-after-free vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. **CVE ID : CVE-2020-3962**	0015.html	
Use After Free	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a use-after-free vulnerability in PVNVRAM. A malicious actor with local access to a virtual machine may be able to read privileged information contained in physical memory. **CVE ID : CVE-2020-3963**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/573
Information Exposure	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the EHCI USB controller. A malicious actor with local access to a virtual machine	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be able to read privileged information contained in the hypervisor's memory. Additional conditions beyond the attacker's control need to be present for exploitation to be possible. **CVE ID : CVE-2020-3964**		
Information Exposure	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the XHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine. **CVE ID : CVE-2020-3965**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/575
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	3.7	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a heap-overflow due to a race condition issue in the USB 2.0 controller (EHCI). A malicious actor with local	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3966**		
Out-of-bounds Write	25-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a heap-overflow vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3967**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/577
Out-of-bounds Write	25-06-2020	4.6	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an out-of-bounds write vulnerability in the USB 3.0 controller (xHCI). A malicious actor with local administrative privileges on a virtual machine may be able to exploit this issue to crash the virtual machine's vmx process leading to a denial of service condition or execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3968**		
Off-by-one Error	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an off-by-one heap-overflow vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible.	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3969		
Out-of-bounds Read	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds read vulnerability in the Shader functionality. A malicious actor with non-administrative local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to crash the virtual machine's vmx process leading to a partial denial of service condition. **CVE ID : CVE-2020-3970**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/580
Out-of-bounds Write	25-06-2020	2.1	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201907101-SG), Workstation (15.x before 15.0.2), and Fusion (11.x before 11.0.2) contain a heap overflow vulnerability in the vmxnet3 virtual network adapter. A malicious actor with local access to a virtual machine with a vmxnet3 network adapter present may be able to read privileged information contained in physical memory. **CVE ID : CVE-2020-3971**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-FUSI-070820/581

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cloud_foundation					
Use After Free	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a use-after-free vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. **CVE ID : CVE-2020-3962**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-CLOU-070820/582
Use After Free	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a use-after-free vulnerability in PVNVRAM. A malicious actor with local access to a virtual machine may be able to read privileged information contained in physical memory. **CVE ID : CVE-2020-3963**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-CLOU-070820/583
Information Exposure	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-	https://www.vmware.com/security/advisories/VMSA-	A-VMW-CLOU-070820/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the EHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in the hypervisor's memory. Additional conditions beyond the attacker's control need to be present for exploitation to be possible. **CVE ID : CVE-2020-3964**	2020-0015.html	
Information Exposure	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the XHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine. **CVE ID : CVE-2020-3965**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-CLOU-070820/585
Concurrent Execution using Shared Resource with	25-06-2020	3.7	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-	https://www.vmware.com/security/advisories/VMSA-	A-VMW-CLOU-070820/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a heap-overflow due to a race condition issue in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3966**	2020-0015.html	
Out-of-bounds Write	25-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a heap-overflow vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3967**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-CLOU-070820/587
Out-of-	25-06-2020	4.6	VMware ESXi (7.0 before	https://ww	A-VMW-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds write vulnerability in the USB 3.0 controller (xHCI). A malicious actor with local administrative privileges on a virtual machine may be able to exploit this issue to crash the virtual machine's vmx process leading to a denial of service condition or execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3968**	w.vmware.com/security/advisories/VMSA-2020-0015.html	CLOU-070820/588
Off-by-one Error	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an off-by-one heap-overflow vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-CLOU-070820/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3969**		
Out-of-bounds Read	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds read vulnerability in the Shader functionality. A malicious actor with non-administrative local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to crash the virtual machine's vmx process leading to a partial denial of service condition. **CVE ID : CVE-2020-3970**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-CLOU-070820/590
Out-of-bounds Write	25-06-2020	2.1	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201907101-SG), Workstation (15.x before 15.0.2), and Fusion (11.x before 11.0.2) contain a heap overflow vulnerability in the vmxnet3 virtual network adapter. A malicious actor with local access to a virtual machine with a vmxnet3	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	A-VMW-CLOU-070820/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network adapter present may be able to read privileged information contained in physical memory. **CVE ID : CVE-2020-3971**		
W3C					
css_validator					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	3.5	In CSS Validator less than or equal to commit 54d68a1, there is a cross-site scripting vulnerability in handling URIs. A user would have to click on a specifically crafted validator link to trigger it. This has been patched in commit e5c09a9. **CVE ID : CVE-2020-4070**	https://github.com/w3c/css-validator/security/advisories/GHSA-wf36-7w73-rh8c	A-W3C-CSS_-070820/592
webtareas_project					
webtareas					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-06-2020	4.3	The loginForm within the general/login.php webpage in webTareas 2.0p8 suffers from a Reflected Cross Site Scripting (XSS) vulnerability via the query string. **CVE ID : CVE-2020-14973**	N/A	A-WEB-WEBT-070820/593
winmagic					
securedoc					
Improper Privilege Management	22-06-2020	4.6	The SDDisk2k.sys driver of WinMagic SecureDoc v8.5 and earlier allows local users to read or write to physical disc sectors via a \\.\SecureDocDevice handle. Exploiting this vulnerability results in privileged code	https://www.winmagic.com/support/release-notes/securedoc-v8-5-sr2/, https://ww	A-WIN-SECU-070820/594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-11519**	w.winmagic.com/support/release-notes/securedoc-v8-5-sr2-hf1	
Improper Privilege Management	22-06-2020	4.6	The SDDisk2k.sys driver of WinMagic SecureDoc v8.5 and earlier allows local users to write to arbitrary kernel memory addresses because the IOCTL dispatcher lacks pointer validation. Exploiting this vulnerability results in privileged code execution. **CVE ID : CVE-2020-11520**	https://www.winmagic.com/support/release-notes/securedoc-v8-5-sr2/, https://www.winmagic.com/support/release-notes/securedoc-v8-5-sr2-hf1	A-WIN-SECU-070820/595
Wolfssl					
wolfssl					
Inadequate Encryption Strength	25-06-2020	5	The private-key operations in ecc.c in wolfSSL before 4.4.0 do not use a constant-time modular inverse when mapping to affine coordinates, aka a "projective coordinates leak." **CVE ID : CVE-2020-11735**	https://github.com/wolfSSL/wolfssl/commit/1de07da61f0c8e9926dcbd68119f73230dae283f, https://github.com/wolfSSL/wolfssl/releases/tag/v4.4.0-stable	A-WOL-WOLF-070820/596
Wso2					
identity_server_as_key_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2020	3.5	An issue was discovered in WSO2 Identity Server through 5.9.0 and WSO2 IS as Key Manager through 5.9.0. A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console Policy Administration user interface. **CVE ID : CVE-2020-14444**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0707	A-WSO-IDEN-070820/597
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2020	3.5	An issue was discovered in WSO2 Identity Server through 5.9.0 and WSO2 IS as Key Manager through 5.9.0. A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console Basic Policy Editor user Interface. **CVE ID : CVE-2020-14445**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0711	A-WSO-IDEN-070820/598
URL Redirection to Untrusted Site ('Open Redirect')	18-06-2020	5.8	An issue was discovered in WSO2 Identity Server through 5.10.0 and WSO2 IS as Key Manager through 5.10.0. An open redirect exists. **CVE ID : CVE-2020-14446**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0713	A-WSO-IDEN-070820/599
identity_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2020	3.5	An issue was discovered in WSO2 Identity Server through 5.9.0 and WSO2 IS as Key Manager through 5.9.0. A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0707	A-WSO-IDEN-070820/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Management Console Policy Administration user interface. **CVE ID : CVE-2020-14444**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-06-2020	3.5	An issue was discovered in WSO2 Identity Server through 5.9.0 and WSO2 IS as Key Manager through 5.9.0. A potential Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console Basic Policy Editor user Interface. **CVE ID : CVE-2020-14445**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0711	A-WSO-IDEN-070820/601
URL Redirection to Untrusted Site ('Open Redirect')	18-06-2020	5.8	An issue was discovered in WSO2 Identity Server through 5.10.0 and WSO2 IS as Key Manager through 5.10.0. An open redirect exists. **CVE ID : CVE-2020-14446**	https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2020-0713	A-WSO-IDEN-070820/602
Zammad					
Zammad					
Missing Authorization	16-06-2020	5.5	In Zammad before 3.3.1, a Customer has ticket access that should only be available to an Agent (e.g., read internal data, split, or merge). **CVE ID : CVE-2020-14213**	N/A	A-ZAM-ZAMM-070820/603
Missing Authorization	16-06-2020	5.8	Zammad before 3.3.1, when Domain Based Assignment is enabled, relies on a claimed e-mail address for authorization decisions. An attacker can register a new account that will have access	N/A	A-ZAM-ZAMM-070820/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to all tickets of an arbitrary Organization. **CVE ID : CVE-2020-14214**		
ZTE					
ztemarket_apk					
Information Exposure	17-06-2020	5.5	All versions up to 10.06 of ZTEMarket APK are impacted by an information leak vulnerability. Due to Activity Component exposure users can exploit this vulnerability to get the private cookie and execute silent installation. **CVE ID : CVE-2020-6869**	N/A	A-ZTE-ZTEM-070820/605
Zyxel					
cloudcnm_secumanager					
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account. **CVE ID : CVE-2020-15312**	N/A	A-ZYX-CLOU-070820/606
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded ECDSA SSH key for the root account. **CVE ID : CVE-2020-15313**	N/A	A-ZYX-CLOU-070820/607
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account. **CVE ID : CVE-2020-15314**	N/A	A-ZYX-CLOU-070820/608
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account within the /opt/axess chroot	N/A	A-ZYX-CLOU-070820/609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directory tree. **CVE ID : CVE-2020-15315**		
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded ECDSA SSH key for the root account within the /opt/axess chroot directory tree. **CVE ID : CVE-2020-15316**	N/A	A-ZYX-CLOU-070820/610
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account within the /opt/axess chroot directory tree. **CVE ID : CVE-2020-15317**	N/A	A-ZYX-CLOU-070820/611
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded DSA SSH key for the root account within the /opt/mysql chroot directory tree. **CVE ID : CVE-2020-15318**	N/A	A-ZYX-CLOU-070820/612
Use of Hard-coded Credentials	29-06-2020	4.3	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a hardcoded RSA SSH key for the root account within the /opt/mysql chroot directory tree. **CVE ID : CVE-2020-15319**	N/A	A-ZYX-CLOU-070820/613
Use of Hard-coded Credentials	29-06-2020	7.5	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the axiros password for the root account. **CVE ID : CVE-2020-15320**	N/A	A-ZYX-CLOU-070820/614
Use of Hard-coded	29-06-2020	7.5	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1	N/A	A-ZYX-CLOU-070820/615

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			has the axzyxel password for the livedbuser account. **CVE ID : CVE-2020-15321**		
Use of Hard-coded Credentials	29-06-2020	7.5	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the wbboEZ4BN3ssxAfM hardcoded password for the debian-sys-maint account. **CVE ID : CVE-2020-15322**	N/A	A-ZYX-CLOU-070820/616
Use of Hard-coded Credentials	29-06-2020	7.5	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has the cloud1234 password for the a1@chopin account default credentials. **CVE ID : CVE-2020-15323**	N/A	A-ZYX-CLOU-070820/617
Missing Authentication for Critical Function	26-06-2020	5	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has no authentication for /registerCpe requests. **CVE ID : CVE-2020-15335**	N/A	A-ZYX-CLOU-070820/618
Missing Authentication for Critical Function	26-06-2020	5	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has no authentication for /cnr requests. **CVE ID : CVE-2020-15336**	N/A	A-ZYX-CLOU-070820/619
cloud_cnm_secumanager					
Use of Hard-coded Credentials	29-06-2020	7.5	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 has a world-readable axess/opt/axXMPPHandler/config/xmpp_config.py file that stores hardcoded credentials. **CVE ID : CVE-2020-15324**	N/A	A-ZYX-CLOU-070820/620
Improper Neutralization of Special	26-06-2020	10	Zyxel CloudCNM SecuManager 3.1.0 and 3.1.1 allows use of	N/A	A-ZYX-CLOU-070820/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			live/CPEManager/AXCampaignManager/delete_cpes_by_ids?cpe_ids= for eval injection of Python code. **CVE ID : CVE-2020-15348**		
Operating System					
abus					
secvest_wireless_control_fube50001_firmware					
Information Exposure	17-06-2020	4.8	The wireless-communication feature of the ABUS Secvest FUBE50001 device does not encrypt sensitive data such as PIN codes or IDs of used proximity chip keys (RFID tokens). This makes it easier for an attacker to disarm the wireless alarm system. **CVE ID : CVE-2020-14157**	N/A	O-ABU-SECV-070820/622
aliasrobotics					
mir100_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it	https://github.com/aliasrobotics/RVD/issues/2566	O-ALI-MIR1-070820/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**	https://github.com/aliasrobotics/RVD/issues/2557	O-ALI-MIR1-070820/624
Exposure of Resource to Wrong	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS)	https://github.com/aliasrobotics/R	O-ALI-MIR1-070820/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	VD/issues/2555	
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious	https://github.com/aliasrobotics/RVD/issues/2554	O-ALI-MIR1-070820/626

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	O-ALI-MIR1-070820/627
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-ALI-MIR1-070820/628
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race	https://github.com/aliasrobotics/RVD/issues/2569	O-ALI-MIR1-070820/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**		
mir200_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	O-ALI-MIR2-070820/630
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available	https://github.com/aliasrobotics/RVD/issues/2557	O-ALI-MIR2-070820/631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched	https://github.com/aliasrobotics/RVD/issues/2555	O-ALI-MIR2-070820/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	O-ALI-MIR2-070820/633
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and	https://github.com/aliasrobotics/RVD/issues/2560	O-ALI-MIR2-070820/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. **CVE ID : CVE-2020-10273**		
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-ALI-MIR2-070820/635
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	O-ALI-MIR2-070820/636
mir250_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely	https://github.com/aliasrobotics/RVD/issues/2566	O-ALI-MIR2-070820/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but	https://github.com/aliasrobotics/RVD/issues/2557	O-ALI-MIR2-070820/638

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	https://github.com/aliasrobotics/RVD/issues/2555	O-ALI-MIR2-070820/639
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of	https://github.com/aliasrobotics/RVD/issues/2554	O-ALI-MIR2-070820/640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	O-ALI-MIR2-070820/641
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-ALI-MIR2-070820/642
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system,	https://github.com/aliasrobotics/RVD/issues/	O-ALI-MIR2-070820/643

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	2569	
mir500_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	O-ALI-MIR5-070820/644
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the	https://github.com/aliasrobotics/RVD/issues/	O-ALI-MIR5-070820/645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**	2557	
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate.	https://github.com/aliasrobotics/RVD/issues/2555	O-ALI-MIR5-070820/646

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	O-ALI-MIR5-070820/647
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property	https://github.com/aliasrobotics/RVD/issues/2560	O-ALI-MIR5-070820/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**		
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-ALI-MIR5-070820/649
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	O-ALI-MIR5-070820/650
mir1000_firmware					
Use of Hard-coded	24-06-2020	5	One of the wireless interfaces within MiR100,	https://github.com/alia	O-ALI-MIR1-070820/651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	srobotics/RVD/issues/2566	
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and	https://github.com/aliasrobotics/RVD/issues/2557	O-ALI-MIR1-070820/652

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the	https://github.com/aliasrobotics/RVD/issues/2555	O-ALI-MIR1-070820/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	O-ALI-MIR1-070820/654
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	O-ALI-MIR1-070820/655
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot	https://github.com/aliasrobotics/RVD/issues/2561	O-ALI-MIR1-070820/656

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**		
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	O-ALI-MIR1-070820/657
Apple					
macos					
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9592**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/658
Improper Restriction of Operations within the	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and	https://helpx.adobe.com/security/products/acrobat/aps	O-APP-MACO-070820/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9593**	b20-24.html	
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9594**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/660
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9595**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/661
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security feature bypass. **CVE ID : CVE-2020-9596**		
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9597**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/663
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9598**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/664
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9602**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/665
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166	https://helpx.adobe.com/security	O-APP-MACO-070820/666

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9603**	/products/acrobat/apsb20-24.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9604**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/667
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9605**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/668
Use After Free	25-06-2020	4.6	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2020-9606**		
Use After Free	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9607**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/670
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9608**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/671
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9609**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/672
NULL Pointer Dereference	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166	https://helpx.adobe.com/security/products/	O-APP-MACO-070820/673

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and earlier, and 2015.006.30518 and earlier have a null pointer vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9610**	acrobat/apsb20-24.html	
Uncontrolled Resource Consumption	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9611**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/674
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9612**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/675
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass.	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9613		
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9614**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/677
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	5.1	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a race condition vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9615**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MACO-070820/678
mac_os					
Improper Input Validation	19-06-2020	2.1	VMware Tools for macOS (11.x.x and prior before 11.1.1) contains a denial-of-service vulnerability in the Host-Guest File System (HGFS) implementation. Successful exploitation of this issue may allow attackers with non-admin privileges on guest macOS virtual machines to create a denial-of-service condition on their own VMs. **CVE ID : CVE-2020-3972**	N/A	O-APP-MAC_-070820/679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9599**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MAC_-070820/680
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9600**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MAC_-070820/681
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9601**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-APP-MAC_-070820/682
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/dng-sdk/apsb20	O-APP-MAC_-070820/683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2020-9625**	-26.html	
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9627**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-APP-MAC_-070820/684
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9628**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-APP-MAC_-070820/685
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9662**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	O-APP-MAC_-070820/686
iphone_os					
Information Exposure	19-06-2020	5	An issue was discovered in Mattermost Mobile Apps before 1.29.0. The iOS app allowed Single Sign-On cookies and Local Storage to remain after a logout, aka MMSA-2020-0013. **CVE ID : CVE-2020-14451**	https://mattermost.com/security-updates/	O-APP-IPHO-070820/687
ARM					
mbed_os					
Improper	18-06-2020	6.4	Buffer over-reads were	https://gith	O-ARM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses CoAP input linearly using a while loop. Once an option is parsed in a loop, the current point (*packet_data_pptr) is increased correspondingly. The pointer is restricted by the size of the received buffer, as well as by the option delta and option length bytes. The actual input packet length is not verified against the number of bytes read when processing the option extended delta and the option extended length. Moreover, the calculation of the message_left variable, in the case of non-extended option deltas, is incorrect and indicates more data left for processing than provided in the function input. All of these lead to heap-based or stack-based memory location read access that is outside of the intended boundary of the buffer. Depending on the platform-specific memory management mechanisms, it can lead to processing of unintended inputs or system	ub.com/ARMmbed/mbed-coap/pull/116	MBED-070820/688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory access violation errors. **CVE ID : CVE-2020-12883**		
Out-of-bounds Read	18-06-2020	6.4	A buffer over-read was discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse_multiple_options() parses CoAP options that may occur multiple consecutive times in a single packet. While processing the options, packet_data_pptr is accessed after being incremented by option_len without a prior out-of-bounds memory check. The temp_parsed_uri_query_ptr is validated for a correct range, but the range valid for temp_parsed_uri_query_ptr is derived from the amount of allocated heap memory, not the actual input size. Therefore the check of temp_parsed_uri_query_ptr may be insufficient for safe access to the area pointed to by packet_data_pptr. As a result, access to a memory area outside of the intended boundary of the packet buffer is made. **CVE ID : CVE-2020-12884**	https://github.com/ARMmbed/mbed-coap/pull/116	O-ARM-MBED-070820/689
Loop with Unreachable	18-06-2020	7.8	An infinite loop was discovered in the CoAP	https://github.com/AR	O-ARM-MBED-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse_multiple_options() parses CoAP options in a while loop. This loop's exit condition is computed using the previously allocated heap memory required for storing the result of parsing multiple options. If the input heap memory calculation results in zero bytes, the loop exit condition is never met and the loop is not terminated. As a result, the packet parsing function never exits, leading to resource consumption. **CVE ID : CVE-2020-12885**	Mmbed/mbed-coap/pull/116	070820/690
Out-of-bounds Read	18-06-2020	6.4	A buffer over-read was discovered in the CoAP library in Arm Mbed OS 5.15.3. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses the CoAP packet header starting from the message token. The length of the token in the received message is provided in the first byte parsed by the sn_coap_parser_options_parse() function. The length encoded in the message is not validated against the	https://github.com/ARMmbed/mbed-coap/pull/116	O-ARM-MBED-070820/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			actual input buffer length before accessing the token. As a result, memory access outside of the intended boundary of the buffer may occur. **CVE ID : CVE-2020-12886**		
Improper Release of Memory Before Removing Last Reference	18-06-2020	5	Memory leaks were discovered in the CoAP library in Arm Mbed OS 5.15.3 when using the Arm mbed-coap library 5.1.5. The CoAP parser is responsible for parsing received CoAP packets. The function sn_coap_parser_options_parse() parses the CoAP option number field of all options present in the input packet. Each option number is calculated as a sum of the previous option number and a delta of the current option. The delta and the previous option number are expressed as unsigned 16-bit integers. Due to lack of overflow detection, it is possible to craft a packet that wraps the option number around and results in the same option number being processed again in a single packet. Certain options allocate memory by calling a memory allocation function. In the cases of COAP_OPTION_URI_QUERY, COAP_OPTION_URI_PATH, COAP_OPTION_LOCATION_QUERY, and	https://github.com/ARMmbed/mbed-coap/pull/116	O-ARM-MBED-070820/692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			COAP_OPTION_ETAG, there is no check on whether memory has already been allocated, which in conjunction with the option number integer overflow may lead to multiple assignments of allocated memory to a single pointer. This has been demonstrated to lead to memory leak by buffer orphaning. As a result, the memory is never freed. **CVE ID : CVE-2020-12887**		
asrock					
rgb_driver_firmware					
N/A	29-06-2020	2.1	AsrDrv103.sys in the ASRock RGB Driver does not properly restrict access from user space, as demonstrated by triggering a triple fault via a request to zero CR3. **CVE ID : CVE-2020-15368**	N/A	O-ASR-RGB_-070820/693
baxter					
em2400_firmware					
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems use cleartext messages to communicate order information with an order entry system. This could allow an attacker with network access to view sensitive data including PHI. **CVE ID : CVE-2020-12008**	N/A	O-BAX-EM24-070820/694
Use of Hard-coded	29-06-2020	3.6	Baxter ExactaMix EM 2400 & EM 1200, Versions	N/A	O-BAX-EM24-070820/695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13, and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 have hard-coded administrative account credentials for the ExactaMix application. Successful exploitation of this vulnerability may allow an attacker with physical access to gain unauthorized access to view/update system configuration or data. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI. **CVE ID : CVE-2020-12012**		
Use of Hard-coded Credentials	29-06-2020	10	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 have hard-coded administrative account credentials for the ExactaMix operating system. Successful exploitation of this vulnerability may allow an attacker who has gained unauthorized access to system resources, including	N/A	O-BAX-EM24-070820/696

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to execute software or to view/update files, directories, or system configuration. This could allow an attacker with network access to view sensitive data including PHI. **CVE ID : CVE-2020-12016**		
Exposure of Resource to Wrong Sphere	29-06-2020	3.6	Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13 and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 does not restrict non administrative users from gaining access to the operating system and editing the application startup script. Successful exploitation of this vulnerability may allow an attacker to alter the startup script as the limited-access user. **CVE ID : CVE-2020-12020**	N/A	O-BAX-EM24-070820/697
Missing Authorizatio n	29-06-2020	3.6	Baxter ExactaMix EM 2400 versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 does not restrict access to the USB interface from an unauthorized user with physical access. Successful exploitation of this vulnerability may allow an attacker with physical access to the system the ability to load an unauthorized payload or unauthorized access to the hard drive by booting a live USB OS. This	N/A	O-BAX-EM24-070820/698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI. **CVE ID : CVE-2020-12024**		
Missing Encryption of Sensitive Data	29-06-2020	6.4	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems store device data with sensitive information in an unencrypted database. This could allow an attacker with network access to view or modify sensitive data including PHI. **CVE ID : CVE-2020-12032**	N/A	O-BAX-EM24-070820/699
em1200_firmware					
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems use cleartext messages to communicate order information with an order entry system. This could allow an attacker with network access to view sensitive data including PHI. **CVE ID : CVE-2020-12008**	N/A	O-BAX-EM12-070820/700
Use of Hard-coded Credentials	29-06-2020	3.6	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13, and ExactaMix EM1200 Versions	N/A	O-BAX-EM12-070820/701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.1, 1.2, and 1.4 have hard-coded administrative account credentials for the ExactaMix application. Successful exploitation of this vulnerability may allow an attacker with physical access to gain unauthorized access to view/update system configuration or data. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI. **CVE ID : CVE-2020-12012**		
Use of Hard-coded Credentials	29-06-2020	10	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 have hard-coded administrative account credentials for the ExactaMix operating system. Successful exploitation of this vulnerability may allow an attacker who has gained unauthorized access to system resources, including access to execute software or to view/update files, directories, or system configuration. This could allow an attacker with network access to view	N/A	O-BAX-EM12-070820/702

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive data including PHI. **CVE ID : CVE-2020-12016**		
Exposure of Resource to Wrong Sphere	29-06-2020	3.6	Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13 and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 does not restrict non administrative users from gaining access to the operating system and editing the application startup script. Successful exploitation of this vulnerability may allow an attacker to alter the startup script as the limited-access user. **CVE ID : CVE-2020-12020**	N/A	O-BAX-EM12-070820/703
Missing Authorizatio n	29-06-2020	3.6	Baxter ExactaMix EM 2400 versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 does not restrict access to the USB interface from an unauthorized user with physical access. Successful exploitation of this vulnerability may allow an attacker with physical access to the system the ability to load an unauthorized payload or unauthorized access to the hard drive by booting a live USB OS. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI.	N/A	O-BAX-EM12-070820/704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12024		
Missing Encryption of Sensitive Data	29-06-2020	6.4	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems store device data with sensitive information in an unencrypted database. This could allow an attacker with network access to view or modify sensitive data including PHI. **CVE ID : CVE-2020-12032**	N/A	O-BAX-EM12-070820/705
prismaflex_firmware					
Use of Hard-coded Credentials	29-06-2020	3.6	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The PrismaFlex device contains a hard-coded service password that provides access to biomedical information, device settings, calibration settings, and network configuration. This could allow an attacker to modify device settings and calibration. **CVE ID : CVE-2020-12035**	N/A	O-BAX-PRIS-070820/706
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record)	N/A	O-BAX-PRIS-070820/707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12036**		
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12037**	N/A	O-BAX-PRIS-070820/708
prismax_firmware					
Use of Hard-coded Credentials	29-06-2020	3.6	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The PrismaFlex device contains a hard-coded service password that provides access to biomedical information, device settings, calibration settings, and network configuration. This could allow an attacker to modify device settings and calibration. **CVE ID : CVE-2020-12035**	N/A	O-BAX-PRIS-070820/709
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit	N/A	O-BAX-PRIS-070820/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12036**		
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12037**	N/A	O-BAX-PRIS-070820/711
phoenix_x36_firmware					
Cleartext Transmission of Sensitive Information	29-06-2020	5	Phoenix Hemodialysis Delivery System SW 3.36 and 3.40, The Phoenix Hemodialysis device does not support data-in-transit encryption (e.g., TLS/SSL) when transmitting treatment and prescription data on the network between the Phoenix system and the Exalis dialysis data management tool. An attacker with access to the network could observe	N/A	O-BAX-PHOE-070820/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive treatment and prescription data sent between the Phoenix system and the Exalis tool. **CVE ID : CVE-2020-12048**		
sigma_spectrum_infusion_system_firmware					
Use of Hard-coded Credentials	29-06-2020	2.1	Baxter Sigma Spectrum Infusion Pumps Sigma Spectrum Infusion System v's6.x model 35700BAX & Baxter Spectrum Infusion System v's8.x model 35700BAX2 contain hardcoded passwords when physically entered on the keypad provide access to biomedical menus including device settings, view calibration values, network configuration of Sigma Spectrum WBM if installed. **CVE ID : CVE-2020-12039**	N/A	O-BAX-SIGM-070820/713
Cleartext Transmission of Sensitive Information	29-06-2020	5	Sigma Spectrum Infusion System v's6.x (model 35700BAX) and Baxter Spectrum Infusion System Version(s) 8.x (model 35700BAX2) at the application layer uses an unauthenticated clear-text communication channel to send and receive system status and operational data. This could allow an attacker that has circumvented network security measures to view sensitive non-private data or to perform a man-in-the-middle attack.	N/A	O-BAX-SIGM-070820/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12040		
Incorrect Permission Assignment for Critical Resource	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) telnet Command-Line Interface, grants access to sensitive data stored on the WBM that permits temporary configuration changes to network settings of the WBM, and allows the WBM to be rebooted. Temporary configuration changes to network settings are removed upon reboot. **CVE ID : CVE-2020-12041**	N/A	O-BAX-SIGM-070820/715
Operation on a Resource after Expiration or Release	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when configured for wireless networking the FTP service operating on the WBM remains operational until the WBM is rebooted. **CVE ID : CVE-2020-12043**	N/A	O-BAX-SIGM-070820/716
Use of Hard-coded Credentials	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when used in conjunction with a Baxter Spectrum v8.x (model 35700BAX2), operates a Telnet service on Port 1023 with hard-coded credentials. **CVE ID : CVE-2020-12045**	N/A	O-BAX-SIGM-070820/717
Use of Hard-coded Credentials	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24), when used with a Baxter Spectrum v8.x (model 35700BAX2) in	N/A	O-BAX-SIGM-070820/718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a factory-default wireless configuration enables an FTP service with hard-coded credentials. **CVE ID : CVE-2020-12047**		
Canonical					
ubuntu_linux					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	2.6	GNU Mailman before 2.1.33 allows arbitrary content injection via the Cgi/private.py private archive login page. **CVE ID : CVE-2020-15011**	N/A	O-CAN-UBUN-070820/719
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-CAN-UBUN-070820/720
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-CAN-UBUN-070820/721
Improper Input Validation	30-06-2020	2.1	NVIDIA Virtual GPU Manager and the guest drivers contain a vulnerability in vGPU plugin, in which there is the	https://nvidia.custhelp.com/app/answers/det	O-CAN-UBUN-070820/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potential to execute privileged operations, which may lead to denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3). **CVE ID : CVE-2020-5973**	ail/a_id/5031	
cellebrite					
ufed_firmware					
Use of Hard-coded Credentials	30-06-2020	5	The Cellebrite UFED physical device 5.0 through 7.5.0.845 relies on key material hardcoded within both the executable code supporting the decryption process, and within the encrypted files themselves by using a key enveloping technique. The recovered key material is the same for every device running the same version of the software, and does not appear to be changed with each new build. It is possible to reconstruct the decryption process using the hardcoded key material and obtain easy access to otherwise protected data. **CVE ID : CVE-2020-14474**	N/A	O-CEL-UFED-070820/723
Cisco					
rv130_firmware					
Improper Restriction of Operations within the Bounds of a	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an	N/A	O-CIS-RV13-070820/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3268**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**	N/A	O-CIS-RV13-070820/725
rv016_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management	N/A	O-CIS-RV01-070820/726

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful	N/A	O-CIS-RV01-070820/727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**	N/A	O-CIS-RV01-070820/728
Improper Neutralization of Special	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	O-CIS-RV01-070820/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The	N/A	O-CIS-RV01-070820/730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending	N/A	O-CIS-RV01-070820/731

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	O-CIS-RV01-070820/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**	N/A	O-CIS-RV01-070820/733
Improper Restriction of	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	O-CIS-RV01-070820/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote	N/A	O-CIS-RV01-070820/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on	N/A	O-CIS-RV01-070820/736

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based	N/A	O-CIS-RV01-070820/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A	N/A	O-CIS-RV01-070820/738

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	O-CIS-RV01-070820/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**	N/A	O-CIS-RV01-070820/740
Improper Restriction of	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	O-CIS-RV01-070820/741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote	N/A	O-CIS-RV01-070820/742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv042_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The	N/A	O-CIS-RV04-070820/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending	N/A	O-CIS-RV04-070820/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**	N/A	O-CIS-RV04-070820/745
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	O-CIS-RV04-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		070820/746
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute	N/A	O-CIS-RV04-070820/747

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management	N/A	O-CIS-RV04-070820/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute	N/A	O-CIS-RV04-070820/749

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**	N/A	O-CIS-RV04-070820/750
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	O-CIS-RV04-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		070820/751
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers	N/A	O-CIS-RV04-070820/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities	N/A	O-CIS-RV04-070820/753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative	N/A	O-CIS-RV04-070820/754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large	N/A	O-CIS-RV04-070820/755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute	N/A	O-CIS-RV04-070820/756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**	N/A	O-CIS-RV04-070820/757
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	O-CIS-RV04-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		070820/758
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers	N/A	O-CIS-RV04-070820/759

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv042g_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute	N/A	O-CIS-RV04-070820/760

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management	N/A	O-CIS-RV04-070820/761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	N/A	O-CIS-RV04-070820/762

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3276		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**	N/A	O-CIS-RV04-070820/763
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an	N/A	O-CIS-RV04-070820/764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with	N/A	O-CIS-RV04-070820/765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could	N/A	O-CIS-RV04-070820/766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	O-CIS-RV04-070820/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**	N/A	O-CIS-RV04-070820/768
Improper Restriction of	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	O-CIS-RV04-070820/769

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote	N/A	O-CIS-RV04-070820/770

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on	N/A	O-CIS-RV04-070820/771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based	N/A	O-CIS-RV04-070820/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A	N/A	O-CIS-RV04-070820/773

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	O-CIS-RV04-070820/774

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**	N/A	O-CIS-RV04-070820/775
Improper Restriction of	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	O-CIS-RV04-070820/776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv082_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers	N/A	O-CIS-RV08-070820/777

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input	N/A	O-CIS-RV08-070820/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary	N/A	O-CIS-RV08-070820/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**	N/A	O-CIS-RV08-070820/780
Improper Neutralization of Special Elements used in an OS	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco	N/A	O-CIS-RV08-070820/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management	N/A	O-CIS-RV08-070820/782

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large	N/A	O-CIS-RV08-070820/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute	N/A	O-CIS-RV08-070820/784

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**	N/A	O-CIS-RV08-070820/785
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	O-CIS-RV08-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		070820/786
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers	N/A	O-CIS-RV08-070820/787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities	N/A	O-CIS-RV08-070820/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative	N/A	O-CIS-RV08-070820/789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large	N/A	O-CIS-RV08-070820/790

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute	N/A	O-CIS-RV08-070820/791

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**	N/A	O-CIS-RV08-070820/792
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	O-CIS-RV08-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		070820/793
unified_ip_phone_6901_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote	N/A	O-CIS-UNIF-070820/794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_6961_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful	N/A	O-CIS-UNIF-070820/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_6945_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/796
unified_ip_phone_6941_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and	N/A	O-CIS-UNIF-070820/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_6921_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow	N/A	O-CIS-UNIF-070820/798

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_6911_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/799
unified_ip_phone_7832_firmware					
Information	18-06-2020	5	A vulnerability in the Web	N/A	O-CIS-UNIF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		070820/800
unified_ip_phone_7861_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending	N/A	O-CIS-UNIF-070820/801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7841_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
unified_ip_phone_7821_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/803
unified_ip_phone_7811_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker	N/A	O-CIS-UNIF-070820/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7937g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device.	N/A	O-CIS-UNIF-070820/805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3360		
unified_ip_phone_7975g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/806
unified_ip_phone_7965g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an	N/A	O-CIS-UNIF-070820/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7962g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of	N/A	O-CIS-UNIF-070820/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7961g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/809
unified_ip_phone_7960g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access	N/A	O-CIS-UNIF-070820/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7945g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain	N/A	O-CIS-UNIF-070820/811

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7942g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/812
unified_ip_phone_7941g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected	N/A	O-CIS-UNIF-070820/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7940g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive	N/A	O-CIS-UNIF-070820/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7931g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/815
unified_ip_phone_7911g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote	N/A	O-CIS-UNIF-070820/816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7906g_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful	N/A	O-CIS-UNIF-070820/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8811_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/818
unified_ip_phone_8841_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and	N/A	O-CIS-UNIF-070820/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8845_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow	N/A	O-CIS-UNIF-070820/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8851_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/821
unified_ip_phone_8851nr_firmware					
Information	18-06-2020	5	A vulnerability in the Web	N/A	O-CIS-UNIF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		070820/822
unified_ip_phone_8861_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending	N/A	O-CIS-UNIF-070820/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8865_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
unified_ip_phone_8865nr_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/825
unified_ip_phone_8961_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker	N/A	O-CIS-UNIF-070820/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8945_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device.	N/A	O-CIS-UNIF-070820/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3360		
unified_ip_phone_8941_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	O-CIS-UNIF-070820/828
unified_ip_phone_9971_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an	N/A	O-CIS-UNIF-070820/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_9951_firmware					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of	N/A	O-CIS-UNIF-070820/830

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. **CVE ID : CVE-2020-3360**		
staros					
Improper Input Validation	18-06-2020	5	A vulnerability in the Enhanced Charging Service (ECS) functionality of Cisco ASR 5000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass the traffic classification rules on an affected device. The vulnerability is due to insufficient input validation of user traffic going through an affected device. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to bypass the traffic classification rules and potentially avoid being charged for traffic consumption. **CVE ID : CVE-2020-3244**	N/A	O-CIS-STAR-070820/831
asyncos					
Improper Input Validation	18-06-2020	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. The vulnerability is due to	N/A	O-CIS-ASYN-070820/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of URLs. An attacker could exploit this vulnerability by crafting the URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for the affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2020-3368**		
rv320_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the	N/A	O-CIS-RV32-070820/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**	N/A	O-CIS-RV32-070820/834
Improper Neutralization of Special Elements	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325	N/A	O-CIS-RV32-070820/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because	N/A	O-CIS-RV32-070820/836

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an	N/A	O-CIS-RV32-070820/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**	N/A	O-CIS-RV32-070820/838
Improper Restriction	18-06-2020	9	Multiple vulnerabilities in the web-based management	N/A	O-CIS-RV32-070820/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an	N/A	O-CIS-RV32-070820/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient	N/A	O-CIS-RV32-070820/841

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient	N/A	O-CIS-RV32-070820/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device,	N/A	O-CIS-RV32-070820/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root	N/A	O-CIS-RV32-070820/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**	N/A	O-CIS-RV32-070820/845
Improper Restriction	18-06-2020	9	Multiple vulnerabilities in the web-based management	N/A	O-CIS-RV32-070820/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an	N/A	O-CIS-RV32-070820/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient	N/A	O-CIS-RV32-070820/848

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient	N/A	O-CIS-RV32-070820/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv325_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an	N/A	O-CIS-RV32-070820/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**	N/A	O-CIS-RV32-070820/851
Improper Neutralizatio	18-06-2020	9	Multiple vulnerabilities in the web-based management	N/A	O-CIS-RV32-070820/852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an	N/A	O-CIS-RV32-070820/853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each	N/A	O-CIS-RV32-070820/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**	N/A	O-CIS-RV32-070820/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**	N/A	O-CIS-RV32-070820/856
Improper Restriction of Operations within the Bounds of a	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016,	N/A	O-CIS-RV32-070820/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected	N/A	O-CIS-RV32-070820/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An	N/A	O-CIS-RV32-070820/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests	N/A	O-CIS-RV32-070820/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow	N/A	O-CIS-RV32-070820/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**	N/A	O-CIS-RV32-070820/862

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**	N/A	O-CIS-RV32-070820/863
Improper Restriction of Operations within the Bounds of a	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016,	N/A	O-CIS-RV32-070820/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected	N/A	O-CIS-RV32-070820/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An	N/A	O-CIS-RV32-070820/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv110w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3268**	N/A	O-CIS-RV11-070820/867
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote	N/A	O-CIS-RV11-070820/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**		
rv130w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3268**	N/A	O-CIS-RV13-070820/869
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**	N/A	O-CIS-RV13-070820/870

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rv215w_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3268**	N/A	O-CIS-RV21-070820/871
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**	N/A	O-CIS-RV21-070820/872
ios_xr					
Incorrect Authorization	18-06-2020	5	A vulnerability in the access control list (ACL) functionality of the standby route processor management interface of Cisco IOS XR Software could allow an unauthenticated,	N/A	O-CIS-IOS_-070820/873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to reach the configured IP addresses on the standby route processor management Gigabit Ethernet Management interface. The vulnerability is due to a logic error that was introduced in the Cisco IOS XR Software, which prevents the ACL from working when applied against the standby route processor management interface. An attacker could exploit this vulnerability by attempting to access the device through the standby route processor management interface. **CVE ID : CVE-2020-3364**		
Debian					
debian_linux					
Use After Free	29-06-2020	5.8	jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be triggered if there is a mix of valid and invalid files in a directory operated on by the decompressor. Triggering a double-free may also be possible. This is related to calling opj_image_destroy twice. **CVE ID : CVE-2020-15389**	N/A	O-DEB-DEBI-070820/874
Improper Neutralization of Special Elements in Output Used	21-06-2020	4.3	Mutt before 1.14.4 and NeoMutt before 2020-06-19 have a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a	N/A	O-DEB-DEBI-070820/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			server sends a "begin TLS" response, the client reads additional data (e.g., from a man-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-14954**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	2.6	GNU Mailman before 2.1.33 allows arbitrary content injection via the Cgi/private.py private archive login page. **CVE ID : CVE-2020-15011**	N/A	O-DEB-DEBI-070820/876
Improper Initialization	29-06-2020	5	In coturn before version 4.5.1.3, there is an issue whereby STUN/TURN response buffer is not initialized properly. There is a leak of information between different client connections. One client (an attacker) could use their connection to intelligently query coturn to get interesting bytes in the padding bytes from the connection of another client. This has been fixed in 4.5.1.3. **CVE ID : CVE-2020-4067**	https://github.com/coturn/coturn/security/advisories/GHSA-c8r8-8vp5-6gcm	O-DEB-DEBI-070820/877
Deserialization of Untrusted Data	19-06-2020	5	A deserialization of untrusted data vulnerability exists in rails < 5.2.4.3, rails < 6.0.3.1 which can allow an attacker to supply information can be	N/A	O-DEB-DEBI-070820/878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inadvertently leaked fromStrong Parameters. **CVE ID : CVE-2020-8164**		
Deserialization of Untrusted Data	19-06-2020	7.5	A deserialization of untrusted data vulnernerability exists in rails < 5.2.4.3, rails < 6.0.3.1 that can allow an attacker to unmarshal user-provided objects in MemCacheStore and RedisCacheStore potentially resulting in an RCE. **CVE ID : CVE-2020-8165**	https://weblog.rubyonrails.org/2020/5/18/Rails-5-2-4-3-and-6-0-3-1-have-been-released/	O-DEB-DEBI-070820/879
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-06-2020	5	Apache Traffic Server 6.0.0 to 6.2.3, 7.0.0 to 7.1.10, and 8.0.0 to 8.0.7 is vulnerable to certain types of HTTP/2 HEADERS frames that can cause the server to allocate a large amount of memory and spin the thread. **CVE ID : CVE-2020-9494**	https://lists.apache.org/thread.html/rf7f86917f42fdaf904d99560cba0c016e03baea6244c47efeb60ecbe%40%3Cdev.trafficserver.apache.org%3E	O-DEB-DEBI-070820/880
Dell					
powermax_os					
Missing Authorization	23-06-2020	5.5	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an authorization bypass vulnerability. An authenticated malicious user	https://www.dell.com/support/security/en-us/details/544585/DSA-2020-065-Dell-EMC-Unisphere-	O-DEL-POWE-070820/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may potentially execute commands to alter or stop database statistics. **CVE ID : CVE-2020-5345**	for-PowerMax-Dell-EMC-Unisphere-for-PowerMax-Virtual-Appliance	
Improper Certificate Validation	23-06-2020	6.8	Dell EMC Unisphere for PowerMax versions prior to 9.1.0.17, Dell EMC Unisphere for PowerMax Virtual Appliance versions prior to 9.1.0.17, and PowerMax OS Release 5978 contain an improper certificate validation vulnerability. An unauthenticated remote attacker may potentially exploit this vulnerability to carry out a man-in-the-middle attack by supplying a crafted certificate and intercepting the victim's traffic to view or modify a victim's data in transit. **CVE ID : CVE-2020-5367**	https://www.dell.com/support/security/en-us/details/544585/DSA-2020-065-Dell-EMC-Unisphere-for-PowerMax-Dell-EMC-Unisphere-for-PowerMax-Virtual-Appliance	O-DEL-POWE-070820/882
Draytek					
vigor2960_firmware					
Improper Control of Generation of Code ('Code Injection')	24-06-2020	7.5	On Draytek Vigor3900, Vigor2960, and Vigor 300B devices before 1.5.1.1, there are some command-injection vulnerabilities in the mainfunction.cgi file. **CVE ID : CVE-2020-14472**	N/A	O-DRA-VIGO-070820/883
Out-of-bounds Write	24-06-2020	7.5	Stack-based buffer overflow vulnerability in Vigor3900, Vigor2960, and Vigor300B	https://www.draytek.com/about/s	O-DRA-VIGO-070820/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with firmware before 1.5.1.1. **CVE ID : CVE-2020-14473**	ecurity-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	
Out-of-bounds Write	23-06-2020	7.5	A stack-based buffer overflow on DrayTek Vigor2960, Vigor3900, and Vigor300B devices before 1.5.1.1 allows remote attackers to execute arbitrary code via the formuserphonenumber parameter in an authusersms action to mainfunction.cgi. **CVE ID : CVE-2020-14993**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	O-DRA-VIGO-070820/885
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-06-2020	7.5	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-	N/A	O-DRA-VIGO-070820/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-14472. **CVE ID : CVE-2020-15415**		
vigor300b_firmware					
Improper Control of Generation of Code ('Code Injection')	24-06-2020	7.5	On Draytek Vigor3900, Vigor2960, and Vigor 300B devices before 1.5.1.1, there are some command-injection vulnerabilities in the mainfunction.cgi file. **CVE ID : CVE-2020-14472**	N/A	O-DRA-VIGO-070820/887
Out-of-bounds Write	24-06-2020	7.5	Stack-based buffer overflow vulnerability in Vigor3900, Vigor2960, and Vigor300B with firmware before 1.5.1.1. **CVE ID : CVE-2020-14473**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	O-DRA-VIGO-070820/888
Out-of-bounds Write	23-06-2020	7.5	A stack-based buffer overflow on DrayTek Vigor2960, Vigor3900, and Vigor300B devices before 1.5.1.1 allows remote attackers to execute arbitrary code via the formuserphonenumber parameter in an authusersms action to mainfunction.cgi. **CVE ID : CVE-2020-14993**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-	O-DRA-VIGO-070820/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				overflow-vulnerability-(cve-2020-14473)	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-06-2020	7.5	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472. **CVE ID : CVE-2020-15415**	N/A	O-DRA-VIGO-070820/890
vigor3900_firmware					
Improper Control of Generation of Code ('Code Injection')	24-06-2020	7.5	On Draytek Vigor3900, Vigor2960, and Vigor 300B devices before 1.5.1.1, there are some command-injection vulnerabilities in the mainfunction.cgi file. **CVE ID : CVE-2020-14472**	N/A	O-DRA-VIGO-070820/891
Out-of-bounds Write	24-06-2020	7.5	Stack-based buffer overflow vulnerability in Vigor3900, Vigor2960, and Vigor300B with firmware before 1.5.1.1. **CVE ID : CVE-2020-14473**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerabilit	O-DRA-VIGO-070820/892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				y-(cve-2020-14473)	
Out-of-bounds Write	23-06-2020	7.5	A stack-based buffer overflow on DrayTek Vigor2960, Vigor3900, and Vigor300B devices before 1.5.1.1 allows remote attackers to execute arbitrary code via the formuserphonenumber parameter in an authusersms action to mainfunction.cgi. **CVE ID : CVE-2020-14993**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	O-DRA-VIGO-070820/893
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-06-2020	7.5	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472. **CVE ID : CVE-2020-15415**	N/A	O-DRA-VIGO-070820/894
easyrobotics					
er200_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials	https://github.com/aliasrobotics/RVD/issues/2556	O-EAS-ER20-070820/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**		
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**	https://github.com/aliasrobotics/RVD/issues/2565	O-EAS-ER20-070820/896
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the	https://github.com/aliasrobotics/RVD/issues/2558	O-EAS-ER20-070820/897

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**		
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-EAS-ER20-070820/898
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	O-EAS-ER20-070820/899
er-lite_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw	https://github.com/aliasrobotics/RVD/issues/2556	O-EAS-ER-L-070820/900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**		
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**	https://github.com/aliasrobotics/RVD/issues/2565	O-EAS-ER-L-070820/901
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser	https://github.com/aliasrobotics/RVD/issues/2558	O-EAS-ER-L-070820/902

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**		
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-EAS-ER-L-070820/903
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	O-EAS-ER-L-070820/904
er-flex_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the	https://github.com/aliasrobotics/RVD/issues/2556	O-EAS-ER-F-070820/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**		
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**	https://github.com/aliasrobotics/RVD/issues/2565	O-EAS-ER-F-070820/906
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens)	https://github.com/aliasrobotics/RVD/issues/2558	O-EAS-ER-F-070820/907

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**		
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-EAS-ER-F-070820/908
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	O-EAS-ER-F-070820/909
er-one_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor	https://github.com/aliasrobotics/RVD/issues/2556	O-EAS-ER-O-070820/910

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**		
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**	https://github.com/aliasrobotics/RVD/issues/2565	O-EAS-ER-O-070820/911
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the	https://github.com/aliasrobotics/RVD/issues/2558	O-EAS-ER-O-070820/912

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			safety of the device. **CVE ID : CVE-2020-10276**		
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-EAS-ER-O-070820/913
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	O-EAS-ER-O-070820/914
enabled-robotics					
er-lite_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have	https://github.com/aliasrobotics/RVD/issues/2566	O-ENA-ER-L-070820/915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**	https://github.com/aliasrobotics/RVD/issues/2557	O-ENA-ER-L-070820/916
Exposure of	24-06-2020	5	MiR100, MiR200 and other	https://gith	O-ENA-ER-L-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	ub.com/aliasrobotics/RVD/issues/2555	070820/917
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-	https://github.com/aliasrobotics/RVD/issues/2554	O-ENA-ER-L-070820/918

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	O-ENA-ER-L-070820/919
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-ENA-ER-L-070820/920
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond	https://github.com/aliasrobotics/RVD/issues/2569	O-ENA-ER-L-070820/921

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**		
er-flex_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	O-ENA-ER-F-070820/922
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and	https://github.com/aliasrobotics/RVD/issues/2557	O-ENA-ER-F-070820/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-	https://github.com/aliasrobotics/RVD/issues/2555	O-ENA-ER-F-070820/924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	O-ENA-ER-F-070820/925
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and	https://github.com/aliasrobotics/RVD/issues/2560	O-ENA-ER-F-070820/926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**		
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-ENA-ER-F-070820/927
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	O-ENA-ER-F-070820/928
er-one_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such	https://github.com/aliasrobotics/RVD/issues/2566	O-ENA-ER-O-070820/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly.	https://github.com/aliasrobotics/RVD/issues/2557	O-ENA-ER-O-070820/930

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	https://github.com/aliasrobotics/RVD/issues/2555	O-ENA-ER-O-070820/931
Missing Authentication for Critical	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing	https://github.com/aliasrobotics/RVD/issues/	O-ENA-ER-O-070820/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	2554	
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	O-ENA-ER-O-070820/933
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-ENA-ER-O-070820/934
Incorrect Default	24-06-2020	7.5	MiR robot controllers (central computation unit)	https://github.com/alia	O-ENA-ER-O-070820/935

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	srobotics/RVD/issues/2569	
Fedoraproject					
fedora					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-06-2020	4.3	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway). The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. Ceph versions 3.x and 4.x are vulnerable to this issue. **CVE ID : CVE-2020-10753**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10753	O-FED-FEDO-070820/936
Out-of-bounds Read	25-06-2020	6.8	In libImaging/SgiRleDecode.c in Pillow through 7.0.0, a number of out-of-bounds reads exist in the parsing of SGI image files, a different issue than CVE-2020-5311.	N/A	O-FED-FEDO-070820/937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11538		
Uncontrolled Resource Consumption	18-06-2020	4.3	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. **CVE ID : CVE-2020-14422**	N/A	O-FED-FEDO-070820/938
Information Exposure	24-06-2020	2.6	In MediaWiki before 1.31.8, 1.32.x and 1.33.x before 1.33.4, and 1.34.x before 1.34.2, private wikis behind a caching server using the img_auth.php image authorization security feature may have had their files cached publicly, so any unauthorized user could view them. This occurs because Cache-Control and Vary headers were mishandled. **CVE ID : CVE-2020-15005**	https://gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/core/+/REL1_31/RELEASE-NOTES-1.31, https://gerrit.wikimedia.org/r/plugins/gitiles/mediawiki/core/+/REL1_33/RELEASE-NOTES-1.33, https://lists.wikimedia.org/piperm	O-FED-FEDO-070820/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ail/wikitech-l/2020-June/093535.html	
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	30-06-2020	6.5	An issue was discovered in http/ContentLengthInterpreter.cc in Squid before 4.12 and 5.x before 5.0.3. A Request Smuggling and Poisoning attack can succeed against the HTTP cache. The client sends an HTTP request with a Content-Length header containing "+\ "-" or an uncommon shell whitespace character prefix to the length field-value. **CVE ID : CVE-2020-15049**	https://github.com/squid-cache/squid/security/advisories/GHSA-qf3v-rc95-96j5	O-FED-FEDO-070820/940
Improper Resource Shutdown or Release	17-06-2020	4	In ISC BIND9 versions BIND 9.11.14 -> 9.11.19, BIND 9.14.9 -> 9.14.12, BIND 9.16.0 -> 9.16.3, BIND Supported Preview Edition 9.11.14-S1 -> 9.11.19-S1: Unless a nameserver is providing authoritative service for one or more zones and at least one zone contains an empty non-terminal entry containing an asterisk ("*") character, this defect cannot be encountered. A would-be attacker who is allowed to change zone content could theoretically introduce such a record in order to exploit this condition to cause denial of service, though we	https://kb.isc.org/docs/cve-2020-8619, https://security.netapp.com/advisory/ntap-20200625-0003/	O-FED-FEDO-070820/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			consider the use of this vector unlikely because any such attack would require a significant privilege level and be easily traceable. **CVE ID : CVE-2020-8619**		
Google					
android					
Improper Privilege Management	16-06-2020	7.5	This is an unbounded write into kernel global memory, via a user-controlled buffer size.Product: AndroidVersions: Android kernelAndroid ID: A-135130450 **CVE ID : CVE-2020-0223**	N/A	O-GOO-ANDR-070820/942
Use After Free	16-06-2020	7.5	Function abc_pcie_issue_dma_xfer_sync creates a transfer object, adds it to the session object then continues to work with it. A concurrent thread could retrieve created transfer object from the session object and delete it using abc_pcie_dma_user_xfer_clean. If this happens, abc_pcie_start_dma_xfer and abc_pcie_wait_dma_xfer in the original thread will trigger UAF when working with the transfer object.Product: AndroidVersions: Android kernelAndroid ID: A-151453714 **CVE ID : CVE-2020-0232**	N/A	O-GOO-ANDR-070820/943
Out-of-bounds	16-06-2020	4.6	In crus_afe_get_param of msm-cirrus-playback.c,	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-148189280 **CVE ID : CVE-2020-0234**		070820/944
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-06-2020	7.5	In crus_sp_shared_ioctl we first copy 4 bytes from userdata into "size" variable, and then use that variable as the size parameter for "copy_from_user", ending up overwriting memory following "crus_sp_hdr". "crus_sp_hdr" is a static variable, of type "struct crus_sp_ioctl_header".Product: AndroidVersions: Android kernelAndroid ID: A-135129430 **CVE ID : CVE-2020-0235**	N/A	O-GOO-ANDR-070820/945
Honeywell					
controledge_plc_firmware					
Cleartext Transmission of Sensitive Information	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes a session token on the network. **CVE ID : CVE-2020-10624**	N/A	O-HON-CONT-070820/946
Cleartext Transmissio	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and	N/A	O-HON-CONT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Sensitive Information			RTU (R101, R110, R140, R150, and R151) exposes unencrypted passwords on the network. **CVE ID : CVE-2020-10628**		070820/947
controledge_rtu_firmware					
Cleartext Transmission of Sensitive Information	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes a session token on the network. **CVE ID : CVE-2020-10624**	N/A	O-HON-CONT-070820/948
Cleartext Transmission of Sensitive Information	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes unencrypted passwords on the network. **CVE ID : CVE-2020-10628**	N/A	O-HON-CONT-070820/949
HP					
hp-ux					
N/A	16-06-2020	5	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081. **CVE ID : CVE-2020-4310**	https://www.ibm.com/support/pages/node/6223914	O-HP-HP-U-070820/950
Improper Certificate Validation	16-06-2020	4	IBM MQ Appliance and IBM MQ AMQP Channels 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD do not correctly block or allow clients based on the certificate distinguished name SSLPEER setting. IBM	https://www.ibm.com/support/pages/node/5736885	O-HP-HP-U-070820/951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 177403. **CVE ID : CVE-2020-4320**		
Huawei					
p30_pro_firmware					
Improper Validation of Integrity Check Value	18-06-2020	2.1	HUAWEI P30 and HUAWEI P30 Pro with versions earlier than 10.1.0.135(C00E135R2P11) and versions earlier than 10.1.0.135(C00E135R2P8) have an insufficient integrity check vulnerability. The system does not check certain software package's integrity sufficiently. Successful exploit could allow an attacker to load a crafted software package to the device. **CVE ID : CVE-2020-1834**	N/A	O-HUA-P30_-070820/952
p30_firmware					
Improper Validation of Integrity Check Value	18-06-2020	2.1	HUAWEI P30 and HUAWEI P30 Pro with versions earlier than 10.1.0.135(C00E135R2P11) and versions earlier than 10.1.0.135(C00E135R2P8) have an insufficient integrity check vulnerability. The system does not check certain software package's integrity sufficiently. Successful exploit could allow an attacker to load a crafted software package to the device. **CVE ID : CVE-2020-1834**	N/A	O-HUA-P30_-070820/953
mate_30_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-06-2020	3.3	HUAWEI Mate 30 with versions earlier than 10.1.0.126(C00E125R5P3) have an information disclosure vulnerability. A logic judgment error occurs when the system handling Bluetooth connections, an attacker could craft as an authenticated Bluetooth peer to launch the attack. Successful exploit could cause information disclosure. **CVE ID : CVE-2020-1835**	N/A	O-HUA-MATE-070820/954
fusionsphere_openstack					
Improper Privilege Management	18-06-2020	4.6	FusionSphere OpenStack 6.5.1 have an improper permissions management vulnerability. The software does not correctly perform a privilege assignment when an actor attempts to perform an action. Successful exploit could allow certain user to do certain operations beyond its privilege. **CVE ID : CVE-2020-9225**	N/A	O-HUA-FUSI-070820/955
Iball					
wrb303n_firmware					
Cross-Site Request Forgery (CSRF)	29-06-2020	4.3	iBall WRB303N devices allow CSRF attacks, as demonstrated by enabling remote management, enabling DHCP, or modifying the subnet range for IP addresses. **CVE ID : CVE-2020-15043**	N/A	O-IBA-WRB3-070820/956

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
IBM					
AIX					
N/A	16-06-2020	5	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081. **CVE ID : CVE-2020-4310**	https://www.ibm.com/support/pages/node/6223914	O-IBM-AIX-070820/957
Improper Certificate Validation	16-06-2020	4	IBM MQ Appliance and IBM MQ AMQP Channels 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD do not correctly block or allow clients based on the certificate distinguished name SSLPEER setting. IBM X-Force ID: 177403. **CVE ID : CVE-2020-4320**	https://www.ibm.com/support/pages/node/5736885	O-IBM-AIX-070820/958
kuka					
kr_c4_firmware					
N/A	16-06-2020	3.6	Critical services for operation can be terminated from windows task manager, bringing the manipulator to a halt. After this a Re-Calibration of the brakes needs to be performed. Be noted that this only can be accomplished either by a Kuka technician or by Kuka issued calibration hardware that interfaces with the manipulator furthering the delay and increasing operational costs. **CVE ID : CVE-2020-10268**	https://github.com/aliasrobotics/RVD/issues/2550	O-KUK-KR_C-070820/959
Linux					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
linux_kernel					
Missing Release of Resource after Effective Lifetime	29-06-2020	2.1	In the Linux kernel through 5.7.6, usbtest_disconnect in drivers/usb/misc/usbtest.c has a memory leak, aka CID-28ebeb8db770. **CVE ID : CVE-2020-15393**	N/A	O-LIN-LINU-070820/960
Use After Free	18-06-2020	4.7	In the Linux kernel before 5.4.16, a race condition in tty->disc_data handling in the slip and slcan line discipline could lead to a use-after-free, aka CID-0ace17d56824. This affects drivers/net/slip/slip.c and drivers/net/can/slcan.c. **CVE ID : CVE-2020-14416**	N/A	O-LIN-LINU-070820/961
N/A	16-06-2020	5	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081. **CVE ID : CVE-2020-4310**	https://www.ibm.com/support/pages/node/6223914	O-LIN-LINU-070820/962
Improper Certificate Validation	16-06-2020	4	IBM MQ Appliance and IBM MQ AMQP Channels 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD do not correctly block or allow clients based on the certificate distinguished name SSLPEER setting. IBM X-Force ID: 177403. **CVE ID : CVE-2020-4320**	https://www.ibm.com/support/pages/node/5736885	O-LIN-LINU-070820/963
Out-of-bounds Read	25-06-2020	4.3	Adobe Campaign Classic before 20.2 have an out-of-bounds read vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/c	O-LIN-LINU-070820/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to information disclosure. **CVE ID : CVE-2020-9666**	ampaign/apsb20-34.html	
maipu					
mp1800x-50_firmware					
Information Exposure	29-06-2020	5	The web interface of Maipu MP1800X-50 7.5.3.14(R) devices allows remote attackers to obtain sensitive information via the form/formDeviceVerGet URI, such as system id, hardware model, hardware version, bootloader version, software version, software image file, compilation time, and system uptime. This is similar to CVE-2019-1653. **CVE ID : CVE-2020-13896**	N/A	O-MAI-MP18-070820/965
mi					
mijia_inkjet_printer_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	7.5	An issue was discovered on Xiaomi Mi Jia ink-jet printer < 3.4.6_0138. Injecting parameters to ippserver through the web management background, resulting in command execution vulnerabilities. **CVE ID : CVE-2020-10561**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=13	O-MI-MIJI-070820/966
xiaomi_r3600_firmware					
Information Exposure	24-06-2020	5	An unsafe configuration of nginx lead to information leak in Xiaomi router R3600 ROM before 1.0.50.	https://privacy.mi.com/trust#/security/vulnerability-	O-MI-XIAO-070820/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11959	management/vulnerability-announcement/detail?id=14	
N/A	24-06-2020	7.5	Xiaomi router R3600 ROM before 1.0.50 is affected by a vulnerability when checking backup file in c_upload interface let attacker able to extract malicious file under any location in /tmp, lead to possible RCE and DoS **CVE ID : CVE-2020-11960**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=15	O-MI-XIAO-070820/968
Information Exposure	24-06-2020	5	Xiaomi router R3600 ROM before 1.0.50 is affected by a sensitive information leakage caused by an insecure interface get_config_result without authentication **CVE ID : CVE-2020-11961**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=16	O-MI-XIAO-070820/969
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	7.5	In Xiaomi router R3600, ROM version<1.0.20, the connection service can be injected through the web interface, resulting in stack overflow or remote code execution. **CVE ID : CVE-2020-14094**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=17&locale=zh	O-MI-XIAO-070820/970

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	7.5	In Xiaomi router R3600, ROM version<1.0.20, a connect service suffers from an injection vulnerability through the web interface, leading to a stack overflow or remote code execution. **CVE ID : CVE-2020-14095**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=18&locale=en	O-MI-XIAO-070820/971
Microsoft					
windows					
Incorrect Default Permissions	26-06-2020	7.2	IDrive before 6.7.3.19 on Windows installs by default to %PROGRAMFILES(X86)%\IDriveWindows with weak folder permissions granting any user modify permission (i.e., NT AUTHORITY\Authenticated Users:(OI)(CI)(M)) to the contents of the directory and its sub-folders. In addition, the program installs a service called IDriveService that runs as LocalSystem. Thus, any standard user can escalate privileges to NT AUTHORITY\SYSTEM by substituting the service's binary with a malicious one. **CVE ID : CVE-2020-15351**	N/A	O-MIC-WIND-070820/972
Information Exposure	26-06-2020	4.3	Adobe Digital Editions versions 4.5.11.187212 and below have a file enumeration (host or local network) vulnerability.	https://helpx.adobe.com/security/products/Digital-	O-MIC-WIND-070820/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-3798**	Editions/apsb20-23.html	
Out-of-bounds Read	26-06-2020	4.3	Adobe After Effects versions 17.0.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure . **CVE ID : CVE-2020-3809**	https://helpx.adobe.com/security/products/after_effects/apsb20-21.html	O-MIC-WIND-070820/974
N/A	16-06-2020	5	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081. **CVE ID : CVE-2020-4310**	https://www.ibm.com/support/pages/node/6223914	O-MIC-WIND-070820/975
Improper Certificate Validation	16-06-2020	4	IBM MQ Appliance and IBM MQ AMQP Channels 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD do not correctly block or allow clients based on the certificate distinguished name SSLPEER setting. IBM X-Force ID: 177403. **CVE ID : CVE-2020-4320**	https://www.ibm.com/support/pages/node/5736885	O-MIC-WIND-070820/976
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/50	O-MIC-WIND-070820/977

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5964	38	
Information Exposure	26-06-2020	4.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9553**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/978
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9554**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/979
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9555**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/980
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9556**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/981
Out-of-bounds Read	26-06-2020	4.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9557**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/982

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	26-06-2020	4.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9558**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/983
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9559**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/984
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9560**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/985
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9561**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/986
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9562**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/987
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a heap overflow	https://helpx.adobe.com/security	O-MIC-WIND-070820/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9563**	/products/bridge/apsb20-19.html	
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9564**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/989
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9565**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/990
Use After Free	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9566**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/991
Use After Free	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9567**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/992
Improper Restriction of Operations within the Bounds of a	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/bridge/apsb20-	O-MIC-WIND-070820/993

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			**CVE ID : CVE-2020-9568**	19.html	
Out-of-bounds Write	26-06-2020	9.3	Adobe Bridge versions 10.0.1 and earlier version have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9569**	https://helpx.adobe.com/security/products/bridge/apsb20-19.html	O-MIC-WIND-070820/994
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9570**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	O-MIC-WIND-070820/995
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9571**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	O-MIC-WIND-070820/996
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9572**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	O-MIC-WIND-070820/997
Improper Restriction of Operations within the Bounds of a	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/illustrator/apsb20-	O-MIC-WIND-070820/998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			**CVE ID : CVE-2020-9573**	20.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	26-06-2020	9.3	Adobe Illustrator versions 24.0.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9574**	https://helpx.adobe.com/security/products/illustrator/apsb20-20.html	O-MIC-WIND-070820/999
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9575**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	O-MIC-WIND-070820/1000
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	26-06-2020	9.3	Adobe Character Animator versions 3.2 and earlier have a buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9586**	https://helpx.adobe.com/security/products/character_animator/apsb20-25.html	O-MIC-WIND-070820/1001
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9589**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1002
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could	https://helpx.adobe.com/security/products/dng-	O-MIC-WIND-070820/1003

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to arbitrary code execution. **CVE ID : CVE-2020-9590**	sdk/apsb20-26.html	
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9592**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1004
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9593**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1005
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9594**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1006
Improper Restriction	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042	https://helpx.adobe.co	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9595**	m/security /products/ acrobat/aps b20-24.html	070820/1007
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9596**	https://hel px.adobe.co m/security /products/ acrobat/aps b20-24.html	O-MIC-WIND-070820/1008
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9597**	https://hel px.adobe.co m/security /products/ acrobat/aps b20-24.html	O-MIC-WIND-070820/1009
Improper Restriction of Operations within the Bounds of a Memory	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an invalid memory	https://hel px.adobe.co m/security /products/ acrobat/aps b20-24.html	O-MIC-WIND-070820/1010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			access vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9598**		
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9599**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1011
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9600**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1012
Out-of-bounds Read	25-06-2020	5	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9601**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9602**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1014
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9603**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1015
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9604**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1016
Improper Restriction of Operations within the Bounds of a	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb20-	O-MIC-WIND-070820/1017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			have a buffer error vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9605**	24.html	
Use After Free	25-06-2020	4.6	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9606**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1018
Use After Free	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9607**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1019
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9608**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1020

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9609**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1021
NULL Pointer Dereference	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a null pointer vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9610**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1022
Uncontrolled Resource Consumption	25-06-2020	4.3	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a stack exhaustion vulnerability. Successful exploitation could lead to application denial-of-service. **CVE ID : CVE-2020-9611**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1023
Out-of-bounds Write	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier	https://helpx.adobe.com/security/products/acrobat/apsb20-	O-MIC-WIND-070820/1024

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9612**	24.html	
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9613**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1025
Improper Privilege Management	25-06-2020	6.8	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a security bypass vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9614**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1026
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	5.1	Adobe Acrobat and Reader versions 2020.006.20042 and earlier, 2017.011.30166 and earlier, 2017.011.30166 and earlier, and 2015.006.30518 and earlier have a race condition vulnerability. Successful exploitation could lead to security feature bypass. **CVE ID : CVE-2020-9615**	https://helpx.adobe.com/security/products/acrobat/apsb20-24.html	O-MIC-WIND-070820/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	26-06-2020	4.3	Adobe Premiere Pro versions 14.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9616**	https://helpx.adobe.com/security/products/premiere_pro/apsb20-27.html	O-MIC-WIND-070820/1028
Out-of-bounds Read	26-06-2020	4.3	Adobe Premiere Rush versions 1.5.8 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9617**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-29.html	O-MIC-WIND-070820/1029
Out-of-bounds Read	25-06-2020	4.3	Adobe Audition versions 13.0.5 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9618**	https://helpx.adobe.com/security/products/audition/apsb20-28.html	O-MIC-WIND-070820/1030
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9620**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1031
Out-of-bounds Write	26-06-2020	9.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9621**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1032
Out-of-	26-06-2020	4.3	Adobe DNG Software	https://hel	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9622**	px.adobe.com/security/products/dng-sdk/apsb20-26.html	070820/1033
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9623**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1034
Out-of-bounds Read	26-06-2020	4.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9624**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1035
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9625**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1036
Out-of-bounds Read	26-06-2020	4.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1037

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9626		
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9627**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1038
Out-of-bounds Read	26-06-2020	5	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9628**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1039
Out-of-bounds Read	26-06-2020	4.3	Adobe DNG Software Development Kit (SDK) 1.5 and earlier versions have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9629**	https://helpx.adobe.com/security/products/dng-sdk/apsb20-26.html	O-MIC-WIND-070820/1040
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9637**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	O-MIC-WIND-070820/1041
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have a heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/after_effects/apsb20-	O-MIC-WIND-070820/1042

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9638	35.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9639**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	O-MIC-WIND-070820/1043
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9640**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	O-MIC-WIND-070820/1044
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9641**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	O-MIC-WIND-070820/1045
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-06-2020	9.3	Adobe Illustrator versions 24.1.2 and earlier have a buffer errors vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9642**	https://helpx.adobe.com/security/products/illustrator/apsb20-37.html	O-MIC-WIND-070820/1046
Out-of-bounds Read	25-06-2020	9.3	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution .	https://helpx.adobe.com/security/products/premiere_pro/apsb20-	O-MIC-WIND-070820/1047

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9652	38.html	
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9653**	https://helpx.adobe.com/security/products/premiere_pro/apsb20-38.html	O-MIC-WIND-070820/1048
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Pro versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9654**	https://helpx.adobe.com/security/products/premiere_pro/apsb20-38.html	O-MIC-WIND-070820/1049
Out-of-bounds Read	25-06-2020	9.3	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9655**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-39.html	O-MIC-WIND-070820/1050
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9656**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-39.html	O-MIC-WIND-070820/1051
Out-of-bounds Write	25-06-2020	9.3	Adobe Premiere Rush versions 1.5.12 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9657**	https://helpx.adobe.com/security/products/premiere_rush/apsb20-39.html	O-MIC-WIND-070820/1052
Out-of-bounds	25-06-2020	9.3	Adobe Audition versions 13.0.6 and earlier have an	https://helpx.adobe.co	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9658**	m/security /products/ audition/ap sb20-40.html	070820/1053
Out-of-bounds Write	25-06-2020	9.3	Adobe Audition versions 13.0.6 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9659**	https://helpx.adobe.com/security/products/audition/apsb20-40.html	O-MIC-WIND-070820/1054
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9660**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	O-MIC-WIND-070820/1055
Out-of-bounds Read	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9661**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	O-MIC-WIND-070820/1056
Out-of-bounds Write	25-06-2020	9.3	Adobe After Effects versions 17.1 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9662**	https://helpx.adobe.com/security/products/after_effects/apsb20-35.html	O-MIC-WIND-070820/1057
Out-of-bounds Read	25-06-2020	4.3	Adobe Campaign Classic before 20.2 have an out-of-bounds read vulnerability. Successful exploitation could lead to information	https://helpx.adobe.com/security/products/campaign/ap	O-MIC-WIND-070820/1058

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disclosure. **CVE ID : CVE-2020-9666**	sb20-34.html	
Mitsubishielectric					
melsec_iq-r_firmware					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	O-MIT-MELS-070820/1059
melsec_iq-f_firmware					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	O-MIT-MELS-070820/1060
melsec-q_firmware					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors.	N/A	O-MIT-MELS-070820/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5594		
melsec-l_firmware					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	O-MIT-MELS-070820/1062
melsec-fx_firmware					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	O-MIT-MELS-070820/1063
mobile-industrial-robotics					
er200_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX)	https://github.com/aliasrobotics/RVD/issues/2566	O-MOB-ER20-070820/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it	https://github.com/aliasrobotics/RVD/issues/2557	O-MOB-ER20-070820/1065

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	https://github.com/aliasrobotics/RVD/issues/2555	O-MOB-ER20-070820/1066
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows	https://github.com/aliasrobotics/RVD/issues/2554	O-MOB-ER20-070820/1067

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	O-MOB-ER20-070820/1068
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-MOB-ER20-070820/1069
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses,	https://github.com/aliasrobotics/RVD/issues/2569	O-MOB-ER20-070820/1070

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**		
mobile-industrial-robots					
mir100_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	O-MOB-MIR1-070820/1071
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string	https://github.com/aliasrobotics/RVD/issues/2565	O-MOB-MIR1-070820/1072

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	O-MOB-MIR1-070820/1073
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the	https://github.com/aliasrobotics/RVD/issues/2562	O-MOB-MIR1-070820/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			machine. **CVE ID : CVE-2020-10277**		
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	O-MOB-MIR1-070820/1075
mir200_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	O-MOB-MIR2-070820/1076
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An	https://github.com/aliasrobotics/RVD/issues/2565	O-MOB-MIR2-070820/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	O-MOB-MIR2-070820/1078
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-MOB-MIR2-070820/1079

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	O-MOB-MIR2-070820/1080
mir250_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	O-MOB-MIR2-070820/1081
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to	https://github.com/aliasrobotics/RVD/issues/2565	O-MOB-MIR2-070820/1082

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	O-MOB-MIR2-070820/1083
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-MOB-MIR2-070820/1084
Improper Resource Shutdown or	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a	https://github.com/aliasrobotics/R	O-MOB-MIR2-070820/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release			DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	VD/issues/2568	
mir500_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	O-MOB-MIR5-070820/1086
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete	https://github.com/aliasrobotics/RVD/issues/2565	O-MOB-MIR5-070820/1087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	O-MOB-MIR5-070820/1088
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-MOB-MIR5-070820/1089
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the	https://github.com/aliasrobotics/RVD/issues/2568	O-MOB-MIR5-070820/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the dashboard. **CVE ID : CVE-2020-10280**		
mir1000_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	O-MOB-MIR1-070820/1091
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**	https://github.com/aliasrobotics/RVD/issues/2565	O-MOB-MIR1-070820/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	O-MOB-MIR1-070820/1093
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-MOB-MIR1-070820/1094
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	O-MOB-MIR1-070820/1095

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Netapp					
hci_h610s_firmware					
Use of Hard-coded Credentials	29-06-2020	4	The NetApp HCI H610C, H615C and H610S Baseboard Management Controllers (BMC) are shipped with a documented default account and password that should be changed during the initial node setup. During upgrades to Element 11.8 and 12.0 or the Compute Firmware Bundle 12.2.92 the BMC account password on the H610C, H615C and H610S platforms is reset to the default documented value which could allow remote attackers to cause a Denial of Service (DoS). **CVE ID : CVE-2020-8573**	N/A	O-NET-HCI_-070820/1096
Netgear					
mr60_firmware					
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-MR60-070820/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**		
ms60_firmware					
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-MS60-070820/1098
srk60_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-	O-NET-SRK6-070820/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	on-Some-WiFi-Systems-PSV-2020-0026	
srk60b03_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	O-NET-SRK6-070820/1100
srk60b04_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	O-NET-SRK6-070820/1101
srk60b05_firmware					
Improper	18-06-2020	5.8	Certain NETGEAR devices	https://kb.	O-NET-SRK6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	070820/1102
srk60b06_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	O-NET-SRK6-070820/1103
srr60_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-	O-NET-SRR6-070820/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	Injection-on-Some-WiFi-Systems-PSV-2020-0026	
srs60_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	O-NET-SRS6-070820/1105
rbk752_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25.	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	O-NET-RBK7-070820/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14433		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBK7-070820/1107
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBK7-070820/1108
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061940/Security	O-NET-RBK7-070820/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBK7-070820/1110
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-	O-NET-RBK7-070820/1111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBK7-070820/1112
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-	O-NET-RBK7-070820/1113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBK7-070820/1114
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBK7-070820/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBK7-070820/1116
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBK7-070820/1117
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of	https://kb.netgear.co	O-NET-RBK7-070820/1118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	m/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBK7-070820/1119
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-	O-NET-RBK7-070820/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	Injection-on-Some-WiFi-Systems-PSV-2020-0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBK7-070820/1121
rbk753_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-	O-NET-RBK7-070820/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBK7-070820/1123
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25.	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBK7-070820/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14436		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBK7-070820/1125
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBK7-070820/1126
Improper Neutralization of Special	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/0000619	O-NET-RBK7-070820/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	42/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBK7-070820/1128
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-	O-NET-RBK7-070820/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBK7-070820/1130
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBK7-070820/1131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**		
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBK7-070820/1132
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBK7-070820/1133

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25. **CVE ID : CVE-2020-14430**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBK7-070820/1134
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBK7-070820/1135
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061946/Security	O-NET-RBK7-070820/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBK7-070820/1137
rbk753s_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authenticat	O-NET-RBK7-070820/1138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	ion-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBK7-070820/1139
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	O-NET-RBK7-070820/1140

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	PSV-2020-0039	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBK7-070820/1141
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBK7-070820/1142

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14438		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	O-NET-RBK7-070820/1143
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBK7-070820/1144
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials.	https://kb.netgear.com/0000619	O-NET-RBK7-070820/1145

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	31/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBK7-070820/1146
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-	O-NET-RBK7-070820/1147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	WiFi-Systems-PSV-2020-0044	
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBK7-070820/1148
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-	O-NET-RBK7-070820/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	PSV-2020-0051	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBK7-070820/1150
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBK7-070820/1151

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	O-NET-RBK7-070820/1152
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBK7-070820/1153
rbr750_firmware					
Improper Neutralization of Special	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated	https://kb.netgear.com/0000619	O-NET-RBR7-070820/1154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	32/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBR7-070820/1155
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-	O-NET-RBR7-070820/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	Injection-on-Some-WiFi-Systems-PSV-2020-0039	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBR7-070820/1157
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	O-NET-RBR7-070820/1158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	PSV-2020-0063	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	O-NET-RBR7-070820/1159
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBR7-070820/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14440		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	O-NET-RBR7-070820/1161
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBR7-070820/1162
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before	https://kb.netgear.com/000061936/Security-Advisory-	O-NET-RBR7-070820/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBR7-070820/1164
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-	O-NET-RBR7-070820/1165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBR7-070820/1166
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBR7-070820/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	O-NET-RBR7-070820/1168
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBR7-070820/1169

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rbs750_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	O-NET-RBS7-070820/1170
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBS7-070820/1171
Improper Neutralization of Special Elements in Output Used	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before	https://kb.netgear.com/000061933/Security-Advisory-	O-NET-RBS7-070820/1172

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBS7-070820/1173
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-	O-NET-RBS7-070820/1174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	Injection-on-Some-WiFi-Systems-PSV-2020-0063	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	O-NET-RBS7-070820/1175
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	O-NET-RBS7-070820/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	O-NET-RBS7-070820/1177
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBS7-070820/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBS7-070820/1179
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBS7-070820/1180
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of	https://kb.netgear.co	O-NET-RBS7-070820/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	m/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBS7-070820/1182
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-	O-NET-RBS7-070820/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	Forgery-on-Some-WiFi-Systems-PSV-2020-0049	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	O-NET-RBS7-070820/1184
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-	O-NET-RBS7-070820/1185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	0103	
rbk852_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	O-NET-RBK8-070820/1186
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBK8-070820/1187

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBK8-070820/1188
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBK8-070820/1189
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061941/Security	O-NET-RBK8-070820/1190

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	O-NET-RBK8-070820/1191
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-	O-NET-RBK8-070820/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	O-NET-RBK8-070820/1193
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBK8-070820/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBK8-070820/1195
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBK8-070820/1196

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25. **CVE ID : CVE-2020-14429**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBK8-070820/1197
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBK8-070820/1198
Cross-Site Request Forgery	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before	https://kb.netgear.com/0000619	O-NET-RBK8-070820/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	37/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	O-NET-RBK8-070820/1200
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-	O-NET-RBK8-070820/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	Injection-on-Some-WiFi-Systems-PSV-2020-0103	
rbk853_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	O-NET-RBK8-070820/1202
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-	O-NET-RBK8-070820/1203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBK8-070820/1204
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBK8-070820/1205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14437		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBK8-070820/1206
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	O-NET-RBK8-070820/1207
Improper Neutralization of Special	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/0000619	O-NET-RBK8-070820/1208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	43/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	O-NET-RBK8-070820/1209
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-	O-NET-RBK8-070820/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	on-Some-WiFi-Systems-PSV-2020-0042	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBK8-070820/1211
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBK8-070820/1212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBK8-070820/1213
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBK8-070820/1214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14431		
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBK8-070820/1215
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	O-NET-RBK8-070820/1216
Improper Neutralization of Special Elements used in an OS	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before	https://kb.netgear.com/000061947/Security-Advisory-	O-NET-RBK8-070820/1217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	
rbr850_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	O-NET-RBR8-070820/1218
Improper Neutralization of Special Elements in Output Used by a Downstream Component	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-	O-NET-RBR8-070820/1219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	Injection-on-Some-WiFi-Systems-PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBR8-070820/1220
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-	O-NET-RBR8-070820/1221

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBR8-070820/1222
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	O-NET-RBR8-070820/1223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14439		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBR8-070820/1224
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	O-NET-RBR8-070820/1225
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before	https://kb.netgear.com/000061935/Security	O-NET-RBR8-070820/1226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBR8-070820/1227
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-	O-NET-RBR8-070820/1228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	Systems-PSV-2020-0050	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBR8-070820/1229
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-	O-NET-RBR8-070820/1230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBR8-070820/1231
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	O-NET-RBR8-070820/1232

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBR8-070820/1233
rbs850_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	O-NET-RBS8-070820/1234
Improper Neutralization of Special Elements in	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752	https://kb.netgear.com/000061934/Security	O-NET-RBS8-070820/1235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBS8-070820/1236
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-	O-NET-RBS8-070820/1237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	Injection-on-Some-WiFi-Systems-PSV-2020-0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBS8-070820/1238
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	O-NET-RBS8-070820/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBS8-070820/1240
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11.	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	O-NET-RBS8-070820/1241

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14426		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBS8-070820/1242
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBS8-070820/1243
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before	https://kb.netgear.com/000061938/Security-Advisory-	O-NET-RBS8-070820/1244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBS8-070820/1245
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-	O-NET-RBS8-070820/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBS8-070820/1247
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-	O-NET-RBS8-070820/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBS8-070820/1249
rbk842_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25.	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	O-NET-RBK8-070820/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14433		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBK8-070820/1251
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBK8-070820/1252
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061940/Security	O-NET-RBK8-070820/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBK8-070820/1254
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-	O-NET-RBK8-070820/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBK8-070820/1256
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-	O-NET-RBK8-070820/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBK8-070820/1258
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBK8-070820/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBK8-070820/1260
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBK8-070820/1261
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of	https://kb.netgear.co	O-NET-RBK8-070820/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	m/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBK8-070820/1263
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-	O-NET-RBK8-070820/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	Injection-on-Some-WiFi-Systems-PSV-2020-0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBK8-070820/1265
rbr840_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-	O-NET-RBR8-070820/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBR8-070820/1267
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25.	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	O-NET-RBR8-070820/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14436		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBR8-070820/1269
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBR8-070820/1270
Improper Neutralization of Special	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/0000619	O-NET-RBR8-070820/1271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	42/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBR8-070820/1272
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-	O-NET-RBR8-070820/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBR8-070820/1274
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	O-NET-RBR8-070820/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**		
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBR8-070820/1276
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	O-NET-RBR8-070820/1277

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25. **CVE ID : CVE-2020-14430**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBR8-070820/1278
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBR8-070820/1279
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061946/Security	O-NET-RBR8-070820/1280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBR8-070820/1281
rbs840_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authenticat	O-NET-RBS8-070820/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	ion-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	O-NET-RBS8-070820/1283
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	O-NET-RBS8-070820/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	PSV-2020-0039	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	O-NET-RBS8-070820/1285
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	O-NET-RBS8-070820/1286

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14438		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	O-NET-RBS8-070820/1287
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	O-NET-RBS8-070820/1288
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials.	https://kb.netgear.com/0000619	O-NET-RBS8-070820/1289

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	31/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	O-NET-RBS8-070820/1290
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-	O-NET-RBS8-070820/1291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	WiFi-Systems-PSV-2020-0044	
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-RBS8-070820/1292
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-	O-NET-RBS8-070820/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	PSV-2020-0051	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	O-NET-RBS8-070820/1294
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	O-NET-RBS8-070820/1295

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	O-NET-RBS8-070820/1296
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	O-NET-RBS8-070820/1297
mk62_firmware					
Insufficiently Protected	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials.	https://kb.netgear.com/0000619	O-NET-MK62-070820/1298

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	38/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	
mk63_firmware					
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	O-NET-MK63-070820/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Nvidia					
geforce_firmware					
Improper Privilege Management	24-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-GEFO-070820/1300
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-GEFO-070820/1301
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	O-NVI-GEFO-070820/1302
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode	https://nvidia.custhelp.com/app/answers/det	O-NVI-GEFO-070820/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to denial of service. **CVE ID : CVE-2020-5965**	ail/a_id/5031	
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-GEFO-070820/1304
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-GEFO-070820/1305
quadro_firmware					
Improper Privilege Management	24-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-QUAD-070820/1306

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-QUAD-070820/1307
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	O-NVI-QUAD-070820/1308
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to denial of service. **CVE ID : CVE-2020-5965**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-QUAD-070820/1309
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-QUAD-070820/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-QUAD-070820/1311
tesla_firmware					
Improper Privilege Management	24-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-TESL-070820/1312
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-TESL-070820/1313
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application	https://nvidia.custhelp.com/app/answers/detail/a_id/50	O-NVI-TESL-070820/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	31, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to denial of service. **CVE ID : CVE-2020-5965**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-TESL-070820/1315
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-TESL-070820/1316
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-TESL-070820/1317
nvs_firmware					
Improper	24-06-2020	4.6	NVIDIA Windows GPU	https://nvi	O-NVI-NVS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	dia.custhelp.com/app/answers/detail/a_id/5031	070820/1318
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-NVS_-070820/1319
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	O-NVI-NVS_-070820/1320
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-NVS_-070820/1321

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service. **CVE ID : CVE-2020-5965**		
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-NVS_-070820/1322
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	O-NVI-NVS_-070820/1323
Opensuse					
leap					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	26-06-2020	4.3	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway). The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. Ceph versions 3.x and 4.x are vulnerable to this issue.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10753	O-OPE-LEAP-070820/1324

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10753		
Uncontrolled Resource Consumption	18-06-2020	4.3	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. **CVE ID : CVE-2020-14422**	N/A	O-OPE-LEAP-070820/1325
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of kopano-spamd of openSUSE Leap 15.1, openSUSE Tumbleweed allowed local attackers with the privileges of the kopano user to escalate to root. This issue affects: openSUSE Leap 15.1 kopano-spamd versions prior to 10.0.5-lp151.4.1. openSUSE Tumbleweed kopano-spamd versions prior to 10.0.5-1.1. **CVE ID : CVE-2020-8014**	https://bugzilla.suse.com/show_bug.cgi?id=1164131	O-OPE-LEAP-070820/1326
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo	https://bugzilla.suse.com/show_bug.cgi?id=1169385	O-OPE-LEAP-070820/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8019		
Incorrect Default Permissions	29-06-2020	7.2	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-	https://bugzilla.suse.com/show_bug.cgi?id=1172405	O-OPE-LEAP-070820/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1. **CVE ID : CVE-2020-8022**		
Oracle					
solaris					
N/A	16-06-2020	5	IBM MQ and MQ Appliance 7.1, 7.5, 8.0, 9.0 LTS, 9.1 LTS, and 9.1 C are vulnerable to a denial of service attack due to an error within the Data Conversion logic. IBM X-Force ID: 177081. **CVE ID : CVE-2020-4310**	https://www.ibm.com/support/pages/node/6223914	O-ORA-SOLA-070820/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Certificate Validation	16-06-2020	4	IBM MQ Appliance and IBM MQ AMQP Channels 8.0, 9.0 LTS, 9.1 LTS, and 9.1 CD do not correctly block or allow clients based on the certificate distinguished name SSLPEER setting. IBM X-Force ID: 177403. **CVE ID : CVE-2020-4320**	https://www.ibm.com/support/pages/node/5736885	O-ORA-SOLA-070820/1330
Paloaltonetworks					
pan-os					
Improper Verification of Cryptographic Signature	29-06-2020	9.3	When Security Assertion Markup Language (SAML) authentication is enabled and the 'Validate Identity Provider Certificate' option is disabled (unchecked), improper verification of signatures in PAN-OS SAML authentication enables an unauthenticated network-based attacker to access protected resources. The attacker must have network access to the vulnerable server to exploit this vulnerability. This issue affects PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL). This issue does not affect PAN-OS 7.1. This issue cannot be exploited if SAML is not used for authentication. This issue cannot be exploited if the	https://security.paloaltonetworks.com/CVE-2020-2021	O-PAL-PAN--070820/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Validate Identity Provider Certificate' option is enabled (checked) in the SAML Identity Provider Server Profile. Resources that can be protected by SAML-based single sign-on (SSO) authentication are: GlobalProtect Gateway, GlobalProtect Portal, GlobalProtect Clientless VPN, Authentication and Captive Portal, PAN-OS next-generation firewalls (PA-Series, VM-Series) and Panorama web interfaces, Prisma Access In the case of GlobalProtect Gateways, GlobalProtect Portal, Clientless VPN, Captive Portal, and Prisma Access, an unauthenticated attacker with network access to the affected servers can gain access to protected resources if allowed by configured authentication and Security policies. There is no impact on the integrity and availability of the gateway, portal or VPN server. An attacker cannot inspect or tamper with sessions of regular users. In the worst case, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N). In the case of PAN-OS and		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Panorama web interfaces, this issue allows an unauthenticated attacker with network access to the PAN-OS or Panorama web interfaces to log in as an administrator and perform administrative actions. In the worst-case scenario, this is a critical severity vulnerability with a CVSS Base Score of 10.0 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). If the web interfaces are only accessible to a restricted management network, then the issue is lowered to a CVSS Base Score of 9.6 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). Palo Alto Networks is not aware of any malicious attempts to exploit this vulnerability. **CVE ID : CVE-2020-2021**		
Philips					
clearvue_850_firmware					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the	N/A	O-PHI-CLEA-070820/1332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			alternate service login to view or modify information. **CVE ID : CVE-2020-14477**		
clearvue_350_firmware					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	O-PHI-CLEA-070820/1333
cx50_firmware					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	O-PHI-CX50-070820/1334
affiniti_70_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	O-PHI-AFFI-070820/1335
affiniti_50_firmware					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	O-PHI-AFFI-070820/1336
epiq_7_firmware					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti	N/A	O-PHI-EPIQ-070820/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**		
sparq_firmware					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	O-PHI-SPAR-070820/1338
xperius_firmware					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may	N/A	O-PHI-XPER-070820/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**		
Qualcomm					
qca6574au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1341
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-070820/1342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1343

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1344

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1345
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-QCA6-070820/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
qcs405_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS4-070820/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS4-070820/1348

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS4-070820/1349

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS4-070820/1350

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS4-070820/1351
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS4-070820/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
ipq8074_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-IPQ8-070820/1353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
qca6174a_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1355

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
qca9377_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA9-070820/1356

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA9-070820/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
qca9379_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA9-070820/1358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA9-070820/1359
sdm429w_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	O-QUA-SDM4-070820/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	-2020-bulletin	
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM4-070820/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	lletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1363
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SDM4-070820/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1367
sc7180_firmware					
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before	https://www.qualcomm.com/company/produ	O-QUA-SC71-070820/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	ct-security/bulletins/june-2020-bulletin	
apq8009_firmware					
Buffer Copy	22-06-2020	7.5	Possible buffer overflow	https://ww	O-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1369

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1370
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-APQ8-070820/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1374
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-APQ8-070820/1375

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	bulletin	
apq8098_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1378
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1379

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1380

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1382
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1384

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
msm8953_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1386
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1388

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1389
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to	https://www.qualcomm.com/company/product-	O-QUA-MSM8-070820/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1392

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1393
msm8998_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1395

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1396
Out-of-	22-06-2020	6.4	Possible null-pointer	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	MSM8-070820/1397
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1398

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1400
Out-of-	22-06-2020	7.5	Buffer over-write may occur	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	MSM8-070820/1401
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
nicobar_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-NICO-070820/1403

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-NICO-070820/1404
Out-of-	22-06-2020	4.6	Stack based overflow If the	https://ww	O-QUA-NICO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1405
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-NICO-070820/1406

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
apq8053_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1407

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1408
Improper Privilege Management	22-06-2020	10	Improper access due to socket opened by the logging application without specifying localhost address in Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, Rennell, SDX20	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-APQ8-070820/1409

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3628	bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1410
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1411

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1414
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1415

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1416

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
mdm9207c_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1417

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1418
Improper	22-06-2020	7.5	Possible null-pointer	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	MDM9-070820/1419
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1420

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1422
msm8905_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1423

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3614		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1424
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1428
sdm845_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	O-QUA-SDM8-070820/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	-2020-bulletin	
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SDM8-070820/1430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	lletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM8-070820/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM8-070820/1432
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM8-070820/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM8-070820/1434
Buffer Copy without	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with	https://www.qualcom	O-QUA-SDM8-070820/1435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	m.com/company/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-SDM8-070820/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM8-070820/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
apq8076_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1438

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
apq8017_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1440

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1441
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to	https://www.qualcomm.com/company/product-	O-QUA-APQ8-070820/1442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
apq8096au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1446
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-APQ8-070820/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	lletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1448

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1449
Buffer Copy	22-06-2020	7.5	Buffer overflow will happen	https://ww	O-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1450
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-APQ8-070820/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1452

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1453
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array	https://www.qualcomm.com/com	O-QUA-APQ8-070820/1454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	pany/product-security/bulletins/june-2020-bulletin	
sdm636_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1457
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1460

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1461
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1463

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1464
sdm670_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-SDM6-070820/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3635		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1468
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1469

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3661		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1471
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/june	O-QUA-SDM6-070820/1472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	-2020-bulletin	
sdm710_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM7-070820/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM7-070820/1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM7-070820/1475
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM7-070820/1476

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3642		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM7-070820/1477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/june	O-QUA-SDM7-070820/1478

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM7-070820/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM7-070820/1480
sm6150_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1481

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3614		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1482
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1483

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1484
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1487
Buffer Copy	22-06-2020	7.5	Buffer overflow can occur	https://ww	O-QUA-SM61-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1488
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1489

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM61-070820/1490
qm215_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1491

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3614		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1492
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1493

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1495
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1496

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QM21-070820/1499
sm8150_firmware					
Double Free	22-06-2020	7.2	Double free issue in kernel memory mapping due to lack of memory protection mechanism in Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in SM8150 **CVE ID : CVE-2020-3613**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM81-070820/1500
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SM81-070820/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	lletins/june-2020-bulletin	
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-SM81-070820/1502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM81-070820/1503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM81-070820/1504
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM81-070820/1505

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM81-070820/1506
Buffer Copy	22-06-2020	7.5	Buffer overflow will happen	https://ww	O-QUA-SM81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1507
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-SM81-070820/1508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM81-070820/1509

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM81-070820/1510
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array	https://www.qualcomm.com/com	O-QUA-SM81-070820/1511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	pany/product-security/bulletins/june-2020-bulletin	
mdm9206_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3660		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1515
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-MDM9-070820/1516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1517

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
mdm9607_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1520
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds	https://www.qualcomm.com/company/produ	O-QUA-MDM9-070820/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1523

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
mdm9650_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1525
msm8996au_firmware					
Buffer Copy without	22-06-2020	7.5	Possible buffer overflow while copying the frame to	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/1526

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1527
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3658		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1530
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1531

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1534
mdm9615_firmware					
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
msm8909_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
qca6584au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA6-070820/1537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
qca9886_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCA9-070820/1538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
sdm429_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1540

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1541
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while	https://www.qualcom	O-QUA-SDM4-070820/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	m.com/company/product-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1543

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1545
Out-of-bounds	22-06-2020	7.5	Buffer over-write may occur during fetching track	https://www.qualcom	O-QUA-SDM4-070820/1546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	m.com/company/product-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sdm632_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1549
Out-of-bounds	22-06-2020	4.6	Stack based overflow If the maximum number of	https://www.qualcom	O-QUA-SDM6-070820/1550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	m.com/company/product-security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1551

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1553
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in	https://www.qualcomm.com/company/produ	O-QUA-SDM6-070820/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1555

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1556
msm8917_firmware					
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before	https://www.qualcomm.com/company/produ	O-QUA-MSM8-070820/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	ct-security/bulletins/june-2020-bulletin	
Incorrect Default	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL	https://www.qualcomm.com/com	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	pany/product-security/bulletins/june-2020-bulletin	070820/1558
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1559

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1560
Improper Validation of	22-06-2020	7.5	Possible null-pointer dereference can occur while	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/1561
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1564
Improper Validation of	22-06-2020	4.6	Possible memory corruption in perfservice due to	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/1565
msm8920_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1568
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1569

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1572
msm8937_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1576
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-MSM8-070820/1577

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1579
msm8940_firmware					
Buffer Copy without	22-06-2020	7.5	Possible buffer overflow while copying the frame to	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/1580

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1581
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1582

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3658		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1584
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-MSM8-070820/1585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1586

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
msm8996_firmware					
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1588
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1589

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1590

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1592
sdm450_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1594

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1595
Out-of-	22-06-2020	6.4	Possible null-pointer	https://ww	O-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1596
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1597

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1599
Out-of-	22-06-2020	7.5	Buffer over-write may occur	https://ww	O-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1600
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sm8250_firmware					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM82-070820/1602
Out-of-bounds	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per	https://www.qualcomm.com/com	O-QUA-SM82-070820/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	pany/product-security/bulletins/june-2020-bulletin	
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM82-070820/1604
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table	https://www.qualcomm.com/company/produ	O-QUA-SM82-070820/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	ct-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM82-070820/1606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM82-070820/1607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM82-070820/1608
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size	https://www.qualcomm.com/company/produ	O-QUA-SM82-070820/1609

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	ct-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM82-070820/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sxr2130_firmware					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR2-070820/1611
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	O-QUA-SXR2-070820/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	lletins/june-2020-bulletin	
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR2-070820/1613
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	O-QUA-SXR2-070820/1614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR2-070820/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR2-070820/1616

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR2-070820/1617
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	O-QUA-SXR2-070820/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR2-070820/1619

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sc8180x_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SC81-070820/1620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
qcm2150_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCM2-070820/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCM2-070820/1622
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user	https://www.qualcomm.com/company/produ	O-QUA-QCM2-070820/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	ct-security/bulletins/june-2020-bulletin	
apq8096_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-APQ8-070820/1624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
sda660_firmware					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDA6-070820/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDA6-070820/1626
Improper Validation of	22-06-2020	7.5	Possible null-pointer dereference can occur while	https://www.qualcom	O-QUA-SDA6-070820/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	m.com/company/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDA6-070820/1628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDA6-070820/1629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDA6-070820/1630
sdm439_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1631

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3614		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1632
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1633

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1634

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1635
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1636

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1639
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM4-070820/1640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sdm630_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1642
Out-of-bounds	22-06-2020	4.6	Stack based overflow If the maximum number of	https://www.qualcom	O-QUA-SDM6-070820/1643

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	m.com/company/product-security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1644

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1646
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in	https://www.qualcomm.com/company/produ	O-QUA-SDM6-070820/1647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1649
sdm660_firmware					
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before	https://www.qualcomm.com/company/produ	O-QUA-SDM6-070820/1650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	ct-security/bulletins/june-2020-bulletin	
Incorrect Default	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL	https://www.qualcomm.com/com	O-QUA-SDM6-070820/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	pany/product-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1652

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1653
Improper Validation of	22-06-2020	7.5	Possible null-pointer dereference can occur while	https://www.qualcom	O-QUA-SDM6-070820/1654

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	m.com/company/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1657
Improper Validation of	22-06-2020	4.6	A possible buffer overflow would occur while	https://www.qualcom	O-QUA-SDM6-070820/1658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	m.com/company/product-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDM6-070820/1659

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
mdm9640_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MDM9-070820/1661
msm8909w_firmware					
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before	https://www.qualcomm.com/company/produ	O-QUA-MSM8-070820/1662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	ct-security/bulletins/june-2020-bulletin	
Incorrect Default	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL	https://www.qualcomm.com/com	O-QUA-MSM8-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	pany/product-security/bulletins/june-2020-bulletin	070820/1663
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1664

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1665
Improper Validation of	22-06-2020	7.5	Possible null-pointer dereference can occur while	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/1666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-MSM8-070820/1669
Improper Validation of	22-06-2020	4.6	A possible buffer overflow would occur while	https://www.qualcom	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/1670
qcs605_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1671

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1672

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1673
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple	https://www.qualcomm.com/com	O-QUA-QCS6-070820/1674

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	pany/product-security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1676
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1678

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1679

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-QCS6-070820/1680
sdx20_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDX2-070820/1681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Privilege Management	22-06-2020	10	Improper access due to socket opened by the logging application without specifying localhost address in Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, Rennell, SDX20 **CVE ID : CVE-2020-3628**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDX2-070820/1682
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SDX2-070820/1683

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDX2-070820/1684

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDX2-070820/1685

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDX2-070820/1686
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-SDX2-070820/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SDX2-070820/1688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
sm7150_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1690

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3626		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1691
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1692

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1693
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-SM71-070820/1694

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SM71-070820/1697
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-SM71-070820/1698

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	bulletin	
sxr1130_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR1-070820/1699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR1-070820/1700

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR1-070820/1701
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR1-070820/1702
Out-of-	22-06-2020	6.4	Possible null-pointer	https://ww	O-QUA-SXR1-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1703
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR1-070820/1704

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR1-070820/1705

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SXR1-070820/1706
sdx24_firmware					
Buffer Copy without Checking	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of	https://www.qualcomm.com/com	O-QUA-SDX2-070820/1707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	pany/product-security/bulletins/june-2020-bulletin	
Improper Validation of	22-06-2020	4.6	A possible buffer overflow would occur while	https://www.qualcom	O-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/1708
rennell_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1710

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Improper Privilege Management	22-06-2020	10	Improper access due to socket opened by the logging application without specifying localhost address in Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, Rennell, SDX20 **CVE ID : CVE-2020-3628**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1711
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1712

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1713
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1714

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3660		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1716
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-RENN-070820/1717

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-RENN-070820/1719
saipan_firmware					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	O-QUA-SAIP-070820/1720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SAIP-070820/1721

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SAIP-070820/1722
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SAIP-070820/1723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SAIP-070820/1724
Buffer Copy	22-06-2020	7.5	Buffer overflow will happen	https://ww	O-QUA-SAIP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/1725
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-SAIP-070820/1726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SAIP-070820/1727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-SAIP-070820/1728
ipq6018_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	O-QUA-IPQ6-070820/1729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	bulletin	
kamorta_firmware					
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after	https://www.qualcomm.com/company/product-	O-QUA-KAMO-070820/1730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-KAMO-070820/1731

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3658		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-KAMO-070820/1732
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	O-QUA-KAMO-070820/1733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	O-QUA-KAMO-070820/1734

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
Redhat					
enterprise_linux					
Out-of-bounds Read	26-06-2020	2.1	A buffer over-read flaw was found in RH kernel versions before 5.0 in crypto_authenc_extractkeys in crypto/authenc.c in the IPsec Cryptographic algorithm's module, authenc. When a payload longer than 4 bytes, and is not following 4-byte alignment boundary guidelines, it causes a buffer over-read threat, leading to a system crash. This flaw allows a local attacker with user privileges to cause a denial of service. **CVE ID : CVE-2020-10769**	N/A	O-RED-ENTE-070820/1735
sane-project					
sane_backends					
Out-of-bounds Write	24-06-2020	7.9	A heap buffer overflow in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to execute arbitrary code, aka GHSL-2020-080. **CVE ID : CVE-2020-12861**	https://alioth-lists.debian.net/pipermail/sane-announce/2020/000041.html	O-SAN-SANE-070820/1736
Out-of-bounds Read	24-06-2020	3.3	An out-of-bounds read in SANE Backends before	https://alioth-	O-SAN-SANE-070820/1737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-082. **CVE ID : CVE-2020-12862**	lists.debian.net/pipermail/sane-announce/2020/000041.html	
Out-of-bounds Read	24-06-2020	3.3	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-083. **CVE ID : CVE-2020-12863**	https://alioth-lists.debian.net/pipermail/sane-announce/2020/000041.html	O-SAN-SANE-070820/1738
Use of Uninitialized Resource	24-06-2020	3.3	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-081. **CVE ID : CVE-2020-12864**	https://alioth-lists.debian.net/pipermail/sane-announce/2020/000041.html	O-SAN-SANE-070820/1739
Out-of-bounds Write	24-06-2020	5.2	A heap buffer overflow in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to execute arbitrary code, aka GHSL-2020-084. **CVE ID : CVE-2020-12865**	https://alioth-lists.debian.net/pipermail/sane-announce/2020/000041.html	O-SAN-SANE-070820/1740
NULL Pointer	24-06-2020	2.7	A NULL pointer dereference in SANE Backends before 1.0.30 allows a malicious	https://alioth-lists.debian.	O-SAN-SANE-070820/1741

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			device connected to the same local network as the victim to cause a denial of service, GHSL-2020-079. **CVE ID : CVE-2020-12866**	net/pipermail/sane-announce/2020/000041.html	
satoshilabs					
trezor_model_t_firmware					
Improper Verification of Cryptographic Signature	16-06-2020	4.3	BIP-143 in the Bitcoin protocol specification mishandles the signing of a Segwit transaction, which allows attackers to trick a user into making two signatures in certain cases, potentially leading to a huge transaction fee. NOTE: this affects all hardware wallets. It was fixed in 1.9.1 for the Trezor One and 2.3.1 for the Trezor Model T. **CVE ID : CVE-2020-14199**	N/A	O-SAT-TREZ-070820/1742
trezor_one_firmware					
Improper Verification of Cryptographic Signature	16-06-2020	4.3	BIP-143 in the Bitcoin protocol specification mishandles the signing of a Segwit transaction, which allows attackers to trick a user into making two signatures in certain cases, potentially leading to a huge transaction fee. NOTE: this affects all hardware wallets. It was fixed in 1.9.1 for the Trezor One and 2.3.1 for the Trezor Model T. **CVE ID : CVE-2020-14199**	N/A	O-SAT-TREZ-070820/1743
Schneider-electric					
easergy_t300_firmware					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	16-06-2020	6.8	A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to execute malicious commands on behalf of a legitimate user when xsrf-token data is intercepted. **CVE ID : CVE-2020-7503**	N/A	O-SCH-EASE-070820/1744
Improper Input Validation	16-06-2020	5	A CWE-20: Improper Input Validation vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to disable the webserver service on the device when specially crafted network packets are sent. **CVE ID : CVE-2020-7504**	N/A	O-SCH-EASE-070820/1745
Download of Code Without Integrity Check	16-06-2020	9	A CWE-494 Download of Code Without Integrity Check vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to inject data with dangerous content into the firmware and execute arbitrary code on the system. **CVE ID : CVE-2020-7505**	N/A	O-SCH-EASE-070820/1746
Information Exposure	16-06-2020	5	A CWE-538: File and Directory Information Exposure vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older)	N/A	O-SCH-EASE-070820/1747

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which could allow an attacker to pack or unpack the archive with the firmware for the controller and modules using the usual tar archiver resulting in an information exposure. **CVE ID : CVE-2020-7506**		
Uncontrolled Resource Consumption	16-06-2020	5	A CWE-400: Uncontrolled Resource Consumption vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to login multiple times resulting in a denial of service. **CVE ID : CVE-2020-7507**	N/A	O-SCH-EASE-070820/1748
Improper Restriction of Excessive Authenticati on Attempts	16-06-2020	5	A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to gain full access by brute force. **CVE ID : CVE-2020-7508**	N/A	O-SCH-EASE-070820/1749
Improper Privilege Management	16-06-2020	6.5	A CWE-269: Improper privilege management (write) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to elevate their privileges and delete files. **CVE ID : CVE-2020-7509**	N/A	O-SCH-EASE-070820/1750
N/A	16-06-2020	7.5	A CWE-1103: Use of Platform-Dependent Third	N/A	O-SCH-EASE-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Party Components with vulnerabilities vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to exploit the component. **CVE ID : CVE-2020-7512**		070820/1751
Cleartext Storage of Sensitive Information	16-06-2020	5	A CWE-312: Cleartext Storage of Sensitive Information vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to intercept traffic and read configuration data. **CVE ID : CVE-2020-7513**	N/A	O-SCH-EASE-070820/1752
se					
modicon_m218_firmware					
Out-of-bounds Write	16-06-2020	5	A CWE-787: Out-of-bounds Write vulnerability exists in Modicon M218 Logic Controller (Firmware version 4.3 and prior), which may cause a Denial of Service when specific TCP/IP crafted packets are sent to the Modicon M218 Logic Controller. **CVE ID : CVE-2020-7502**	N/A	O-SE-MODI-070820/1753
easergy_t300_firmware					
Information Exposure	16-06-2020	5	A CWE-200: Information Exposure vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow attacker to obtain private keys. **CVE ID : CVE-2020-7510**	N/A	O-SE-EASE-070820/1754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of a Broken or Risky Cryptographic Algorithm	16-06-2020	5	A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to acquire a password by brute force. **CVE ID : CVE-2020-7511**	N/A	O-SE-EASE-070820/1755
mtn6501-0001_firmware					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	O-SE-MTN6-070820/1756
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	O-SE-MTN6-070820/1757
mtn6501-0002_firmware					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected	N/A	O-SE-MTN6-070820/1758

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	O-SE-MTN6-070820/1759
mtn6260-0410_firmware					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	O-SE-MTN6-070820/1760
Improper Neutralization of Special Elements used in an SQL Command	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions	N/A	O-SE-MTN6-070820/1761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**		
mtn6260-0415_firmware					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	O-SE-MTN6-070820/1762
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	O-SE-MTN6-070820/1763
mtn6260-0310_firmware					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized	N/A	O-SE-MTN6-070820/1764

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	O-SE-MTN6-070820/1765
mtn6260-0315_firmware					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	O-SE-MTN6-070820/1766
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be	N/A	O-SE-MTN6-070820/1767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			executed when a malicious command is entered. **CVE ID : CVE-2020-7500**		
Sophos					
sfos					
Out-of-bounds Write	18-06-2020	7.5	A heap-based buffer overflow in the awarrensmtp component of Sophos XG Firewall v17.5 MR11 and older potentially allows an attacker to run arbitrary code remotely. **CVE ID : CVE-2020-11503**	https://community.sophos.com/b/security-blog/posts/advisory-potential-rce-through-heap-overflow-in-awarrensmtp-cve-2020-11503	O-SOP-SFOS-070820/1768
xg_firewall_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-06-2020	7.5	Sophos XG Firewall 17.x through v17.5 MR12 allows a Buffer Overflow and remote code execution via the HTTP/S Bookmarks feature for clientless access. Hotfix HF062020.1 was published for all firewalls running v17.x. **CVE ID : CVE-2020-15069**	https://community.sophos.com/b/security-blog/posts/advisory-buffer-overflow-vulnerability-in-user-portal	O-SOP-XG_F-070820/1769
Supermicro					
x10drh-it_firmware					
Cross-Site Request Forgery (CSRF)	24-06-2020	9.3	The web interface on Supermicro X10DRH-iT motherboards with BIOS 2.0a and IPMI firmware	N/A	O-SUP-X10D-070820/1770

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			03.40 allows remote attackers to exploit a cgi/config_user.cgi CSRF issue to add new admin users. The fixed versions are BIOS 3.2 and firmware 03.88. **CVE ID : CVE-2020-15046**		
x10drh-it_bios					
Cross-Site Request Forgery (CSRF)	24-06-2020	9.3	The web interface on Supermicro X10DRH-iT motherboards with BIOS 2.0a and IPMI firmware 03.40 allows remote attackers to exploit a cgi/config_user.cgi CSRF issue to add new admin users. The fixed versions are BIOS 3.2 and firmware 03.88. **CVE ID : CVE-2020-15046**	N/A	O-SUP-X10D-070820/1771
Suse					
linux_enterprise_server					
UNIX Symbolic Link (Symlink) Following	29-06-2020	7.2	A UNIX Symbolic Link (Symlink) Following vulnerability in the packaging of syslog-ng of SUSE Linux Enterprise Debuginfo 11-SP3, SUSE Linux Enterprise Debuginfo 11-SP4, SUSE Linux Enterprise Module for Legacy Software 12, SUSE Linux Enterprise Point of Sale 11-SP3, SUSE Linux Enterprise Server 11-SP4-LTSS, SUSE Linux Enterprise Server for SAP 12-SP1; openSUSE Backports SLE-	https://bugzilla.suse.com/show_bug.cgi?id=1169385	O-SUS-LINU-070820/1772

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			15-SP1, openSUSE Leap 15.1 allowed local attackers controlling the user news to escalate their privileges to root. This issue affects: SUSE Linux Enterprise Debuginfo 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Debuginfo 11-SP4 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Module for Legacy Software 12 syslog-ng versions prior to 3.6.4-12.8.1. SUSE Linux Enterprise Point of Sale 11-SP3 syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server 11-SP4-LTSS syslog-ng versions prior to 2.0.9-27.34.40.5.1. SUSE Linux Enterprise Server for SAP 12-SP1 syslog-ng versions prior to 3.6.4-12.8.1. openSUSE Backports SLE-15-SP1 syslog-ng versions prior to 3.19.1-bp151.4.6.1. openSUSE Leap 15.1 syslog-ng versions prior to 3.19.1-lp151.3.6.1. **CVE ID : CVE-2020-8019**		
Incorrect Default Permissions	29-06-2020	7.2	A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux	https://bugzilla.suse.com/show_bug.cgi?id=1172405	O-SUS-LINU-070820/1773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1. **CVE ID : CVE-2020-8022**		
tinxy					
smart_wifi_door_lock_firmware					
Authentication Bypass by Capture-replay	23-06-2020	4.3	Tinxy Door Lock with firmware before 3.2 allow attackers to unlock a door by replaying an Unlock request that occurred when the attacker was previously authorized. In other words, door-access revocation is mishandled. **CVE ID : CVE-2020-9438**	N/A	O-TIN-SMAR-070820/1774
Tp-link					
nc450_firmware					
Buffer Copy without Checking Size of Input ('Classic	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices	N/A	O-TP--NC45-070820/1775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**		
nc260_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	O-TP--NC26-070820/1776
nc250_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through	N/A	O-TP--NC25-070820/1777

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**		
nc230_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	O-TP--NC23-070820/1778
nc220_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	O-TP--NC22-070820/1779
nc210_firmware					
Buffer Copy without	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build	N/A	O-TP--NC21-070820/1780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**		
nc200_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	O-TP--NC20-070820/1781
tl-wr740n_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-06-2020	3.5	On TP-Link TL-WR740N v4 and TL-WR740ND v4 devices, an attacker with access to the admin panel can inject HTML code and change the HTML context of the target pages and stations in the access-control settings via targets_lists_name or	N/A	O-TP--TL-W-070820/1782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hosts_lists_name. The vulnerability can also be exploited through a CSRF, requiring no authentication as an administrator. **CVE ID : CVE-2020-14965**		
tl-wr740nd_firmware					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-06-2020	3.5	On TP-Link TL-WR740N v4 and TL-WR740ND v4 devices, an attacker with access to the admin panel can inject HTML code and change the HTML context of the target pages and stations in the access-control settings via targets_lists_name or hosts_lists_name. The vulnerability can also be exploited through a CSRF, requiring no authentication as an administrator. **CVE ID : CVE-2020-14965**	N/A	O-TP--TL-W-070820/1783
uvd-robots					
uvd_robots_firmware					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the	https://github.com/aliasrobotics/RVD/issues/2566	O-UVD-UVD_-070820/1784

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**	https://github.com/aliasrobotics/RVD/issues/2557	O-UVD-UVD_-070820/1785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	https://github.com/aliasrobotics/RVD/issues/2555	O-UVD-UVD_-070820/1786
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In	https://github.com/aliasrobotics/RVD/issues/2554	O-UVD-UVD_-070820/1787

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	O-UVD-UVD_-070820/1788
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	O-UVD-UVD_-070820/1789
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to	https://github.com/aliasrobotics/RVD/issues/2569	O-UVD-UVD_-070820/1790

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**		
uvd_firmware					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	O-UVD-UVD_-070820/1791
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to	https://github.com/aliasrobotics/RVD/issues/2565	O-UVD-UVD_-070820/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	O-UVD-UVD_-070820/1793
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	O-UVD-UVD_-070820/1794
Improper Resource Shutdown or	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a	https://github.com/aliasrobotics/R	O-UVD-UVD_-070820/1795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release			DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	VD/issues/2568	
Vmware					
esxi					
Use After Free	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a use-after-free vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. **CVE ID : CVE-2020-3962**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1796
Use After Free	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a use-after-free vulnerability in PVNVRAM. A malicious actor with local access to a virtual machine may be able to read privileged information contained in	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			physical memory. **CVE ID : CVE-2020-3963**		
Information Exposure	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the EHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in the hypervisor's memory. Additional conditions beyond the attacker's control need to be present for exploitation to be possible. **CVE ID : CVE-2020-3964**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1798
Information Exposure	25-06-2020	2.1	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202006401-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain an information leak in the XHCI USB controller. A malicious actor with local access to a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			machine. **CVE ID : CVE-2020-3965**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	3.7	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.2), and Fusion (11.x before 11.5.2) contain a heap-overflow due to a race condition issue in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3966**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1800
Out-of-bounds Write	25-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain a heap-overflow vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local access to a virtual machine may be able to exploit this vulnerability to execute code on the hypervisor from a	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1801

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3967**		
Out-of-bounds Write	25-06-2020	4.6	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds write vulnerability in the USB 3.0 controller (xHCI). A malicious actor with local administrative privileges on a virtual machine may be able to exploit this issue to crash the virtual machine's vmx process leading to a denial of service condition or execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3968**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1802
Off-by-one Error	24-06-2020	4.4	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1803

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an off-by-one heap-overflow vulnerability in the SVGA device. A malicious actor with local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to execute code on the hypervisor from a virtual machine. Additional conditions beyond the attacker's control must be present for exploitation to be possible. **CVE ID : CVE-2020-3969**		
Out-of-bounds Read	25-06-2020	1.9	VMware ESXi (7.0 before ESXi_7.0.0-1.20.16321839, 6.7 before ESXi670-202004101-SG and 6.5 before ESXi650-202005401-SG), Workstation (15.x before 15.5.5), and Fusion (11.x before 11.5.5) contain an out-of-bounds read vulnerability in the Shader functionality. A malicious actor with non-administrative local access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to crash the virtual machine's vmx process leading to a partial denial of service condition. **CVE ID : CVE-2020-3970**	https://www.vmware.com/security/advisories/VMSA-2020-0015.html	O-VMW-ESXI-070820/1804
Out-of-bounds Write	25-06-2020	2.1	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201907101-SG),	https://www.vmware.com/security/advisorie	O-VMW-ESXI-070820/1805

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Workstation (15.x before 15.0.2), and Fusion (11.x before 11.0.2) contain a heap overflow vulnerability in the vmxnet3 virtual network adapter. A malicious actor with local access to a virtual machine with a vmxnet3 network adapter present may be able to read privileged information contained in physical memory. **CVE ID : CVE-2020-3971**	s/VMSA-2020-0015.html	
ZTE					
netnumen_u31_r10_firmware					
N/A	24-06-2020	5.2	The version V12.17.20T115 of ZTE U31R20 product is impacted by a design error vulnerability. An attacker could exploit the vulnerability to log in to the FTP server to tamper with the password, and illegally download, modify, upload, or delete files, causing improper operation of the network management system and equipment. This affects: NetNumenU31R20 V12.17.20T115 **CVE ID : CVE-2020-6870**	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1013043	O-ZTE-NETN-070820/1806
Zyxel					
wap6806_firmware					
Improper Limitation of a Pathname to a Restricted	22-06-2020	5	Zyxel Armor X1 WAP6806 1.00(ABAL.6)C0 devices allow Directory Traversal via the images/eaZy/ URI.	N/A	O-ZYX-WAP6-070820/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			**CVE ID : CVE-2020-14461**		
Hardware					
abus					
secvest_wireless_control_fube50001					
Information Exposure	17-06-2020	4.8	The wireless-communication feature of the ABUS Secvest FUBE50001 device does not encrypt sensitive data such as PIN codes or IDs of used proximity chip keys (RFID tokens). This makes it easier for an attacker to disarm the wireless alarm system. **CVE ID : CVE-2020-14157**	N/A	H-ABU-SECV-070820/1808
aliasrobotics					
mir100					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000.	https://github.com/aliasrobotics/RVD/issues/2566	H-ALI-MIR1-070820/1809

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10269		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**	https://github.com/aliasrobotics/RVD/issues/2557	H-ALI-MIR1-070820/1810
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to	https://github.com/aliasrobotics/RVD/issues/2555	H-ALI-MIR1-070820/1811

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot	https://github.com/aliasrobotics/RVD/issues/2554	H-ALI-MIR1-070820/1812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	H-ALI-MIR1-070820/1813
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-ALI-MIR1-070820/1814
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home	https://github.com/aliasrobotics/RVD/issues/2569	H-ALI-MIR1-070820/1815

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**		
mir200					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	H-ALI-MIR2-070820/1816
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and	https://github.com/aliasrobotics/RVD/issues/2557	H-ALI-MIR2-070820/1817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless	https://github.com/aliasrobotics/RVD/issues/2555	H-ALI-MIR2-070820/1818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	H-ALI-MIR2-070820/1819
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data.	https://github.com/aliasrobotics/RVD/issues/2560	H-ALI-MIR2-070820/1820

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10273		
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-ALI-MIR2-070820/1821
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	H-ALI-MIR2-070820/1822
mir250					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX)	https://github.com/aliasrobotics/RVD/issues/2566	H-ALI-MIR2-070820/1823

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it	https://github.com/aliasrobotics/RVD/issues/2557	H-ALI-MIR2-070820/1824

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	https://github.com/aliasrobotics/RVD/issues/2555	H-ALI-MIR2-070820/1825
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows	https://github.com/aliasrobotics/RVD/issues/2554	H-ALI-MIR2-070820/1826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	H-ALI-MIR2-070820/1827
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-ALI-MIR2-070820/1828
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses,	https://github.com/aliasrobotics/RVD/issues/2569	H-ALI-MIR2-070820/1829

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**		
mir500					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	H-ALI-MIR5-070820/1830
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a	https://github.com/aliasrobotics/RVD/issues/2557	H-ALI-MIR5-070820/1831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS	https://github.com/aliasrobotics/RVD/issues/2555	H-ALI-MIR5-070820/1832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	H-ALI-MIR5-070820/1833
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the	https://github.com/aliasrobotics/RVD/issues/2560	H-ALI-MIR5-070820/1834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**		
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-ALI-MIR5-070820/1835
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	H-ALI-MIR5-070820/1836
mir1000					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly	https://github.com/aliasrobotics/R	H-ALI-MIR1-070820/1837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	VD/issues/2566	
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to	https://github.com/aliasrobotics/RVD/issues/2557	H-ALI-MIR1-070820/1838

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS).	https://github.com/aliasrobotics/RVD/issues/2555	H-ALI-MIR1-070820/1839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10271		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	H-ALI-MIR1-070820/1840
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	H-ALI-MIR1-070820/1841
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to	https://github.com/aliasrobotics/RVD/issues/2561	H-ALI-MIR1-070820/1842

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot from a Live Image. **CVE ID : CVE-2020-10278**		
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	H-ALI-MIR1-070820/1843
asrock					
rgb_driver					
N/A	29-06-2020	2.1	AsrDrv103.sys in the ASRock RGB Driver does not properly restrict access from user space, as demonstrated by triggering a triple fault via a request to zero CR3. **CVE ID : CVE-2020-15368**	N/A	H-ASR-RGB_-070820/1844
baxter					
em2400					
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems use cleartext messages to communicate order information with an order entry system. This could allow an attacker with	N/A	H-BAX-EM24-070820/1845

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			network access to view sensitive data including PHI. **CVE ID : CVE-2020-12008**		
Use of Hard-coded Credentials	29-06-2020	3.6	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13, and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 have hard-coded administrative account credentials for the ExactaMix application. Successful exploitation of this vulnerability may allow an attacker with physical access to gain unauthorized access to view/update system configuration or data. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI. **CVE ID : CVE-2020-12012**	N/A	H-BAX-EM24-070820/1846
Use of Hard-coded Credentials	29-06-2020	10	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 have hard-coded administrative account credentials for the	N/A	H-BAX-EM24-070820/1847

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ExactaMix operating system. Successful exploitation of this vulnerability may allow an attacker who has gained unauthorized access to system resources, including access to execute software or to view/update files, directories, or system configuration. This could allow an attacker with network access to view sensitive data including PHI. **CVE ID : CVE-2020-12016**		
Exposure of Resource to Wrong Sphere	29-06-2020	3.6	Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13 and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 does not restrict non administrative users from gaining access to the operating system and editing the application startup script. Successful exploitation of this vulnerability may allow an attacker to alter the startup script as the limited-access user. **CVE ID : CVE-2020-12020**	N/A	H-BAX-EM24-070820/1848
Missing Authorizatio n	29-06-2020	3.6	Baxter ExactaMix EM 2400 versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 does not restrict access to the USB interface from an unauthorized user with physical access. Successful exploitation of this vulnerability may allow an	N/A	H-BAX-EM24-070820/1849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with physical access to the system the ability to load an unauthorized payload or unauthorized access to the hard drive by booting a live USB OS. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI. **CVE ID : CVE-2020-12024**		
Missing Encryption of Sensitive Data	29-06-2020	6.4	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems store device data with sensitive information in an unencrypted database. This could allow an attacker with network access to view or modify sensitive data including PHI. **CVE ID : CVE-2020-12032**	N/A	H-BAX-EM24-070820/1850
em1200					
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems use cleartext messages to communicate order information with an order entry system. This could allow an attacker with network access to view sensitive data including PHI. **CVE ID : CVE-2020-12008**	N/A	H-BAX-EM12-070820/1851
Use of Hard-coded Credentials	29-06-2020	3.6	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions	N/A	H-BAX-EM12-070820/1852

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13, and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 have hard-coded administrative account credentials for the ExactaMix application. Successful exploitation of this vulnerability may allow an attacker with physical access to gain unauthorized access to view/update system configuration or data. This could impact confidentiality and integrity of the system and risk exposure of sensitive information including PHI. **CVE ID : CVE-2020-12012**		
Use of Hard-coded Credentials	29-06-2020	10	Baxter ExactaMix EM 2400 & EM 1200, Versions ExactaMix EM2400 Versions 1.10, 1.11, 1.13, 1.14, ExactaMix EM1200 Versions 1.1, 1.2, 1.4, 1.5, Baxter ExactaMix EM 2400 Versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 have hard-coded administrative account credentials for the ExactaMix operating system. Successful exploitation of this vulnerability may allow an attacker who has gained unauthorized access to system resources, including access to execute software	N/A	H-BAX-EM12-070820/1853

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			or to view/update files, directories, or system configuration. This could allow an attacker with network access to view sensitive data including PHI. **CVE ID : CVE-2020-12016**		
Exposure of Resource to Wrong Sphere	29-06-2020	3.6	Baxter ExactaMix EM 2400 Versions 1.10, 1.11, and 1.13 and ExactaMix EM1200 Versions 1.1, 1.2, and 1.4 does not restrict non administrative users from gaining access to the operating system and editing the application startup script. Successful exploitation of this vulnerability may allow an attacker to alter the startup script as the limited-access user. **CVE ID : CVE-2020-12020**	N/A	H-BAX-EM12-070820/1854
Missing Authorizatio n	29-06-2020	3.6	Baxter ExactaMix EM 2400 versions 1.10, 1.11, 1.13, 1.14 and ExactaMix EM1200 Versions 1.1, 1.2, 1.4 and 1.5 does not restrict access to the USB interface from an unauthorized user with physical access. Successful exploitation of this vulnerability may allow an attacker with physical access to the system the ability to load an unauthorized payload or unauthorized access to the hard drive by booting a live USB OS. This could impact confidentiality	N/A	H-BAX-EM12-070820/1855

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and integrity of the system and risk exposure of sensitive information including PHI. **CVE ID : CVE-2020-12024**		
Missing Encryption of Sensitive Data	29-06-2020	6.4	Baxter ExactaMix EM 2400 Versions 1.10, 1.11 and ExactaMix EM1200 Versions 1.1, 1.2 systems store device data with sensitive information in an unencrypted database. This could allow an attacker with network access to view or modify sensitive data including PHI. **CVE ID : CVE-2020-12032**	N/A	H-BAX-EM12-070820/1856
prismaflex					
Use of Hard-coded Credentials	29-06-2020	3.6	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The PrismaFlex device contains a hard-coded service password that provides access to biomedical information, device settings, calibration settings, and network configuration. This could allow an attacker to modify device settings and calibration. **CVE ID : CVE-2020-12035**	N/A	H-BAX-PRIS-070820/1857
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send	N/A	H-BAX-PRIS-070820/1858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12036**		
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12037**	N/A	H-BAX-PRIS-070820/1859
prismax					
Use of Hard-coded Credentials	29-06-2020	3.6	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The PrismaFlex device contains a hard-coded service password that provides access to biomedical information, device settings, calibration settings, and network configuration. This could allow an attacker to modify device settings and calibration. **CVE ID : CVE-2020-12035**	N/A	H-BAX-PRIS-070820/1860
Cleartext	29-06-2020	5	Baxter PrismaFlex all	N/A	H-BAX-PRIS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Transmission of Sensitive Information			versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12036**		070820/1861
Cleartext Transmission of Sensitive Information	29-06-2020	5	Baxter PrismaFlex all versions, PrisMax all versions prior to 3.x, The affected devices do not implement data-in-transit encryption (e.g., TLS/SSL) when configured to send treatment data to a PDMS (Patient Data Management System) or an EMR (Electronic Medical Record) system. An attacker could observe sensitive data sent from the device. **CVE ID : CVE-2020-12037**	N/A	H-BAX-PRIS-070820/1862
sigma_spectrum_infusion_system					
Use of Hard-coded Credentials	29-06-2020	2.1	Baxter Sigma Spectrum Infusion Pumps Sigma Spectrum Infusion System v's6.x model 35700BAX & Baxter Spectrum Infusion System v's8.x model 35700BAX2 contain hardcoded passwords when physically entered on the keypad provide access to	N/A	H-BAX-SIGM-070820/1863

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			biomedical menus including device settings, view calibration values, network configuration of Sigma Spectrum WBM if installed. **CVE ID : CVE-2020-12039**		
Cleartext Transmission of Sensitive Information	29-06-2020	5	Sigma Spectrum Infusion System v's6.x (model 35700BAX) and Baxter Spectrum Infusion System Version(s) 8.x (model 35700BAX2) at the application layer uses an unauthenticated clear-text communication channel to send and receive system status and operational data. This could allow an attacker that has circumvented network security measures to view sensitive non-private data or to perform a man-in-the-middle attack. **CVE ID : CVE-2020-12040**	N/A	H-BAX-SIGM-070820/1864
Incorrect Permission Assignment for Critical Resource	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) telnet Command-Line Interface, grants access to sensitive data stored on the WBM that permits temporary configuration changes to network settings of the WBM, and allows the WBM to be rebooted. Temporary configuration changes to network settings are removed upon reboot. **CVE ID : CVE-2020-12041**	N/A	H-BAX-SIGM-070820/1865

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operation on a Resource after Expiration or Release	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when configured for wireless networking the FTP service operating on the WBM remains operational until the WBM is rebooted. **CVE ID : CVE-2020-12043**	N/A	H-BAX-SIGM-070820/1866
Use of Hard-coded Credentials	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when used in conjunction with a Baxter Spectrum v8.x (model 35700BAX2), operates a Telnet service on Port 1023 with hard-coded credentials. **CVE ID : CVE-2020-12045**	N/A	H-BAX-SIGM-070820/1867
Use of Hard-coded Credentials	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24), when used with a Baxter Spectrum v8.x (model 35700BAX2) in a factory-default wireless configuration enables an FTP service with hard-coded credentials. **CVE ID : CVE-2020-12047**	N/A	H-BAX-SIGM-070820/1868
wireless_battery_module					
Incorrect Permission Assignment for Critical Resource	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) telnet Command-Line Interface, grants access to sensitive data stored on the WBM that permits temporary configuration changes to network settings of the WBM, and allows the WBM	N/A	H-BAX-WIRE-070820/1869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to be rebooted. Temporary configuration changes to network settings are removed upon reboot. **CVE ID : CVE-2020-12041**		
Operation on a Resource after Expiration or Release	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when configured for wireless networking the FTP service operating on the WBM remains operational until the WBM is rebooted. **CVE ID : CVE-2020-12043**	N/A	H-BAX-WIRE-070820/1870
Use of Hard-coded Credentials	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24) when used in conjunction with a Baxter Spectrum v8.x (model 35700BAX2), operates a Telnet service on Port 1023 with hard-coded credentials. **CVE ID : CVE-2020-12045**	N/A	H-BAX-WIRE-070820/1871
Use of Hard-coded Credentials	29-06-2020	7.5	The Baxter Spectrum WBM (v17, v20D29, v20D30, v20D31, and v22D24), when used with a Baxter Spectrum v8.x (model 35700BAX2) in a factory-default wireless configuration enables an FTP service with hard-coded credentials. **CVE ID : CVE-2020-12047**	N/A	H-BAX-WIRE-070820/1872
phoenix_x36					
Cleartext Transmission of Sensitive Information	29-06-2020	5	Phoenix Hemodialysis Delivery System SW 3.36 and 3.40, The Phoenix Hemodialysis device does	N/A	H-BAX-PHOE-070820/1873

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not support data-in-transit encryption (e.g., TLS/SSL) when transmitting treatment and prescription data on the network between the Phoenix system and the Exalis dialysis data management tool. An attacker with access to the network could observe sensitive treatment and prescription data sent between the Phoenix system and the Exalis tool. **CVE ID : CVE-2020-12048**		
cellebrite					
ufed					
Use of Hard-coded Credentials	30-06-2020	5	The Cellebrite UFED physical device 5.0 through 7.5.0.845 relies on key material hardcoded within both the executable code supporting the decryption process, and within the encrypted files themselves by using a key enveloping technique. The recovered key material is the same for every device running the same version of the software, and does not appear to be changed with each new build. It is possible to reconstruct the decryption process using the hardcoded key material and obtain easy access to otherwise protected data. **CVE ID : CVE-2020-14474**	N/A	H-CEL-UFED-070820/1874
Cisco					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rv320					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**	N/A	H-CIS-RV32-070820/1875
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an	N/A	H-CIS-RV32-070820/1876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with	N/A	H-CIS-RV32-070820/1877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root	N/A	H-CIS-RV32-070820/1878

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**	N/A	H-CIS-RV32-070820/1879
Improper Neutralization of Special Elements used in an OS Command	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016,	N/A	H-CIS-RV32-070820/1880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to	N/A	H-CIS-RV32-070820/1881

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could	N/A	H-CIS-RV32-070820/1882

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could	N/A	H-CIS-RV32-070820/1883

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	H-CIS-RV32-070820/1884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**	N/A	H-CIS-RV32-070820/1885
Improper Restriction of	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	H-CIS-RV32-070820/1886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote	N/A	H-CIS-RV32-070820/1887

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on	N/A	H-CIS-RV32-070820/1888

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based	N/A	H-CIS-RV32-070820/1889

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A	N/A	H-CIS-RV32-070820/1890

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	H-CIS-RV32-070820/1891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3296**		
rv325					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**	N/A	H-CIS-RV32-070820/1892
Improper Neutralization of Special Elements used in an OS Command	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016,	N/A	H-CIS-RV32-070820/1893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly	N/A	H-CIS-RV32-070820/1894

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the	N/A	H-CIS-RV32-070820/1895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**	N/A	H-CIS-RV32-070820/1896
Improper Neutralization of Special Elements	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325	N/A	H-CIS-RV32-070820/1897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient	N/A	H-CIS-RV32-070820/1898

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient	N/A	H-CIS-RV32-070820/1899

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device,	N/A	H-CIS-RV32-070820/1900

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root	N/A	H-CIS-RV32-070820/1901

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**	N/A	H-CIS-RV32-070820/1902
Improper Restriction	18-06-2020	9	Multiple vulnerabilities in the web-based management	N/A	H-CIS-RV32-070820/1903

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an	N/A	H-CIS-RV32-070820/1904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient	N/A	H-CIS-RV32-070820/1905

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient	N/A	H-CIS-RV32-070820/1906

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device,	N/A	H-CIS-RV32-070820/1907

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root	N/A	H-CIS-RV32-070820/1908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv110w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3268**	N/A	H-CIS-RV11-070820/1909
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**	N/A	H-CIS-RV11-070820/1910
rv130w					
Improper Restriction of Operations	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and	N/A	H-CIS-RV13-070820/1911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3268**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**	N/A	H-CIS-RV13-070820/1912
rv215w					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this	N/A	H-CIS-RV21-070820/1913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			advisory. **CVE ID : CVE-2020-3268**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**	N/A	H-CIS-RV21-070820/1914
rv130					
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3268**	N/A	H-CIS-RV13-070820/1915
Improper Restriction of Operations within the Bounds of a	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco RV110W, RV130, RV130W, and RV215W Series Routers could allow an	N/A	H-CIS-RV13-070820/1916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			authenticated, remote attacker with administrative privileges to execute arbitrary commands. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2020-3269**		
rv016					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	N/A	H-CIS-RV01-070820/1917

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3274		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**	N/A	H-CIS-RV01-070820/1918
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an	N/A	H-CIS-RV01-070820/1919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with	N/A	H-CIS-RV01-070820/1920

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root	N/A	H-CIS-RV01-070820/1921

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**	N/A	H-CIS-RV01-070820/1922
Improper Restriction of Operations within the Bounds of a	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016,	N/A	H-CIS-RV01-070820/1923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected	N/A	H-CIS-RV01-070820/1924

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An	N/A	H-CIS-RV01-070820/1925

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests	N/A	H-CIS-RV01-070820/1926

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow	N/A	H-CIS-RV01-070820/1927

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**	N/A	H-CIS-RV01-070820/1928

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**	N/A	H-CIS-RV01-070820/1929
Improper Restriction of Operations within the Bounds of a	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016,	N/A	H-CIS-RV01-070820/1930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected	N/A	H-CIS-RV01-070820/1931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An	N/A	H-CIS-RV01-070820/1932

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests	N/A	H-CIS-RV01-070820/1933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv042					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root	N/A	H-CIS-RV04-070820/1934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**	N/A	H-CIS-RV04-070820/1935
Improper Neutralization of Special Elements used in an OS Command	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016,	N/A	H-CIS-RV04-070820/1936

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly	N/A	H-CIS-RV04-070820/1937

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the	N/A	H-CIS-RV04-070820/1938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**	N/A	H-CIS-RV04-070820/1939
Improper Restriction of Operations	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325	N/A	H-CIS-RV04-070820/1940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative	N/A	H-CIS-RV04-070820/1941

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to	N/A	H-CIS-RV04-070820/1942

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could	N/A	H-CIS-RV04-070820/1943

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could	N/A	H-CIS-RV04-070820/1944

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	H-CIS-RV04-070820/1945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**	N/A	H-CIS-RV04-070820/1946
Improper Restriction of	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	H-CIS-RV04-070820/1947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote	N/A	H-CIS-RV04-070820/1948

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on	N/A	H-CIS-RV04-070820/1949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based	N/A	H-CIS-RV04-070820/1950

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv042g					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful	N/A	H-CIS-RV04-070820/1951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**	N/A	H-CIS-RV04-070820/1952
Improper Neutralization of Special	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	H-CIS-RV04-070820/1953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The	N/A	H-CIS-RV04-070820/1954

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending	N/A	H-CIS-RV04-070820/1955

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3279**	N/A	H-CIS-RV04-070820/1956
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	H-CIS-RV04-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**		070820/1957
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers	N/A	H-CIS-RV04-070820/1958

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities	N/A	H-CIS-RV04-070820/1959

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative	N/A	H-CIS-RV04-070820/1960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large	N/A	H-CIS-RV04-070820/1961

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute	N/A	H-CIS-RV04-070820/1962

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3292**	N/A	H-CIS-RV04-070820/1963
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	H-CIS-RV04-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**		070820/1964
Improper Restriction of Operations within the Bounds of a Memory	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers	N/A	H-CIS-RV04-070820/1965

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities	N/A	H-CIS-RV04-070820/1966

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative	N/A	H-CIS-RV04-070820/1967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
rv082					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending	N/A	H-CIS-RV08-070820/1968

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3274**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3275**	N/A	H-CIS-RV08-070820/1969
Improper	18-06-2020	9	Multiple vulnerabilities in	N/A	H-CIS-RV08-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3276**		070820/1970
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute	N/A	H-CIS-RV08-070820/1971

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3277**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management	N/A	H-CIS-RV08-070820/1972

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system. **CVE ID : CVE-2020-3278**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary commands on an affected device. The vulnerabilities exist because the web-based management interface does not properly validate user-supplied input to scripts. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending malicious requests to an affected device. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the underlying operating system.	N/A	H-CIS-RV08-070820/1973

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3279		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3286**	N/A	H-CIS-RV08-070820/1974
Improper Restriction of Operations	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325	N/A	H-CIS-RV08-070820/1975

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3287**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative	N/A	H-CIS-RV08-070820/1976

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3288**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to	N/A	H-CIS-RV08-070820/1977

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3289**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could	N/A	H-CIS-RV08-070820/1978

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3290**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could	N/A	H-CIS-RV08-070820/1979

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3291**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying	N/A	H-CIS-RV08-070820/1980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. **CVE ID : CVE-2020-3292**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3293**	N/A	H-CIS-RV08-070820/1981
Improper Restriction of	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	N/A	H-CIS-RV08-070820/1982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3294**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote	N/A	H-CIS-RV08-070820/1983

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3295**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-06-2020	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Series Routers and Cisco Small Business RV016, RV042, and RV082 Routers could allow an authenticated, remote attacker with administrative privileges to execute arbitrary code on an affected device. The vulnerabilities are due to insufficient boundary restrictions on	N/A	H-CIS-RV08-070820/1984

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied input to scripts in the web-based management interface. An attacker with administrative privileges that are sufficient to log in to the web-based management interface could exploit each vulnerability by sending crafted requests that contain overly large values to an affected device, causing a stack overflow. A successful exploit could allow the attacker to cause the device to crash or allow the attacker to execute arbitrary code with root privileges on the underlying operating system. **CVE ID : CVE-2020-3296**		
unified_ip_phone_6901					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the	N/A	H-CIS-UNIF-070820/1985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_6961					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/1986
unified_ip_phone_6945					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an	N/A	H-CIS-UNIF-070820/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_6941					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access	N/A	H-CIS-UNIF-070820/1988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_6921					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/1989
unified_ip_phone_6911					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP	N/A	H-CIS-UNIF-070820/1990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7832					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the	N/A	H-CIS-UNIF-070820/1991

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7861					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/1992
unified_ip_phone_7841					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/1993
unified_ip_phone_7821					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this	N/A	H-CIS-UNIF-070820/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7811					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/1995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
unified_ip_phone_7937g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/1996
unified_ip_phone_7975g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker	N/A	H-CIS-UNIF-070820/1997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7965g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device.	N/A	H-CIS-UNIF-070820/1998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3360		
unified_ip_phone_7962g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/1999
unified_ip_phone_7961g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an	N/A	H-CIS-UNIF-070820/2000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7960g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of	N/A	H-CIS-UNIF-070820/2001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7945g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2002
unified_ip_phone_7942g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access	N/A	H-CIS-UNIF-070820/2003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7941g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain	N/A	H-CIS-UNIF-070820/2004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7940g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2005
unified_ip_phone_7931g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected	N/A	H-CIS-UNIF-070820/2006

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7911g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive	N/A	H-CIS-UNIF-070820/2007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_7906g					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2008
unified_ip_phone_8811					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote	N/A	H-CIS-UNIF-070820/2009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8841					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful	N/A	H-CIS-UNIF-070820/2010

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8845					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2011
unified_ip_phone_8851					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and	N/A	H-CIS-UNIF-070820/2012

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8851nr					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow	N/A	H-CIS-UNIF-070820/2013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8861					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2014
unified_ip_phone_8865					
Information	18-06-2020	5	A vulnerability in the Web	N/A	H-CIS-UNIF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		070820/2015
unified_ip_phone_8865nr					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending	N/A	H-CIS-UNIF-070820/2016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_8961					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
unified_ip_phone_8945					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2018
unified_ip_phone_8941					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker	N/A	H-CIS-UNIF-070820/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**		
unified_ip_phone_9971					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device.	N/A	H-CIS-UNIF-070820/2020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3360		
unified_ip_phone_9951					
Information Exposure	18-06-2020	5	A vulnerability in the Web Access feature of Cisco IP Phones Series 7800 and Series 8800 could allow an unauthenticated, remote attacker to view sensitive information on an affected device. The vulnerability is due to improper access controls on the web-based management interface of an affected device. An attacker could exploit this vulnerability by sending malicious requests to the device, which could allow the attacker to bypass access restrictions. A successful attack could allow the attacker to view sensitive information, including device call logs that contain names, usernames, and phone numbers of users of the device. **CVE ID : CVE-2020-3360**	N/A	H-CIS-UNIF-070820/2021
email_security_appliance					
Improper Input Validation	18-06-2020	5	A vulnerability in the antispam protection mechanisms of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to bypass the URL reputation filters on an affected device. The vulnerability is due to	N/A	H-CIS-EMAI-070820/2022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation of URLs. An attacker could exploit this vulnerability by crafting the URL in a particular way. A successful exploit could allow the attacker to bypass the URL reputation filters that are configured for the affected device, which could allow malicious URLs to pass through the device. **CVE ID : CVE-2020-3368**		
asr_5000					
Improper Input Validation	18-06-2020	5	A vulnerability in the Enhanced Charging Service (ECS) functionality of Cisco ASR 5000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass the traffic classification rules on an affected device. The vulnerability is due to insufficient input validation of user traffic going through an affected device. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to bypass the traffic classification rules and potentially avoid being charged for traffic consumption. **CVE ID : CVE-2020-3244**	N/A	H-CIS-ASR_-070820/2023
asr_5500					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	18-06-2020	5	A vulnerability in the Enhanced Charging Service (ECS) functionality of Cisco ASR 5000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass the traffic classification rules on an affected device. The vulnerability is due to insufficient input validation of user traffic going through an affected device. An attacker could exploit this vulnerability by sending a malformed HTTP request to an affected device. A successful exploit could allow the attacker to bypass the traffic classification rules and potentially avoid being charged for traffic consumption. **CVE ID : CVE-2020-3244**	N/A	H-CIS-ASR_-070820/2024
asr_5700					
Improper Input Validation	18-06-2020	5	A vulnerability in the Enhanced Charging Service (ECS) functionality of Cisco ASR 5000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to bypass the traffic classification rules on an affected device. The vulnerability is due to insufficient input validation of user traffic going through an affected device. An attacker could exploit this vulnerability by sending a	N/A	H-CIS-ASR_-070820/2025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malformed HTTP request to an affected device. A successful exploit could allow the attacker to bypass the traffic classification rules and potentially avoid being charged for traffic consumption. **CVE ID : CVE-2020-3244**		
Draytek					
vigor2960					
Improper Control of Generation of Code ('Code Injection')	24-06-2020	7.5	On Draytek Vigor3900, Vigor2960, and Vigor 300B devices before 1.5.1.1, there are some command-injection vulnerabilities in the mainfunction.cgi file. **CVE ID : CVE-2020-14472**	N/A	H-DRA-VIGO-070820/2026
Out-of-bounds Write	24-06-2020	7.5	Stack-based buffer overflow vulnerability in Vigor3900, Vigor2960, and Vigor300B with firmware before 1.5.1.1. **CVE ID : CVE-2020-14473**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	H-DRA-VIGO-070820/2027
Out-of-bounds Write	23-06-2020	7.5	A stack-based buffer overflow on DrayTek Vigor2960, Vigor3900, and Vigor300B devices before	https://www.draytek.com/about/security-	H-DRA-VIGO-070820/2028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.5.1.1 allows remote attackers to execute arbitrary code via the formuserphonenumber parameter in an authusersms action to mainfunction.cgi. **CVE ID : CVE-2020-14993**	advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-06-2020	7.5	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472. **CVE ID : CVE-2020-15415**	N/A	H-DRA-VIGO-070820/2029
vigor300b					
Improper Control of Generation of Code ('Code Injection')	24-06-2020	7.5	On Draytek Vigor3900, Vigor2960, and Vigor 300B devices before 1.5.1.1, there are some command-injection vulnerabilities in the mainfunction.cgi file. **CVE ID : CVE-2020-14472**	N/A	H-DRA-VIGO-070820/2030
Out-of-bounds Write	24-06-2020	7.5	Stack-based buffer overflow vulnerability in Vigor3900, Vigor2960, and Vigor300B with firmware before 1.5.1.1. **CVE ID : CVE-2020-14473**	https://www.draytek.com/about/security-advisory/vigor3900-/-	H-DRA-VIGO-070820/2031

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	
Out-of-bounds Write	23-06-2020	7.5	A stack-based buffer overflow on DrayTek Vigor2960, Vigor3900, and Vigor300B devices before 1.5.1.1 allows remote attackers to execute arbitrary code via the formuserphonenumber parameter in an authusersms action to mainfunction.cgi. **CVE ID : CVE-2020-14993**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	H-DRA-VIGO-070820/2032
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-06-2020	7.5	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472. **CVE ID : CVE-2020-15415**	N/A	H-DRA-VIGO-070820/2033

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
vigor3900					
Improper Control of Generation of Code ('Code Injection')	24-06-2020	7.5	On Draytek Vigor3900, Vigor2960, and Vigor 300B devices before 1.5.1.1, there are some command-injection vulnerabilities in the mainfunction.cgi file. **CVE ID : CVE-2020-14472**	N/A	H-DRA-VIGO-070820/2034
Out-of-bounds Write	24-06-2020	7.5	Stack-based buffer overflow vulnerability in Vigor3900, Vigor2960, and Vigor300B with firmware before 1.5.1.1. **CVE ID : CVE-2020-14473**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-2020-14473)	H-DRA-VIGO-070820/2035
Out-of-bounds Write	23-06-2020	7.5	A stack-based buffer overflow on DrayTek Vigor2960, Vigor3900, and Vigor300B devices before 1.5.1.1 allows remote attackers to execute arbitrary code via the formuserphonenumber parameter in an authusersms action to mainfunction.cgi. **CVE ID : CVE-2020-14993**	https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-stack-based-buffer-overflow-vulnerability-(cve-	H-DRA-VIGO-070820/2036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2020-14473)	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	30-06-2020	7.5	On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472. **CVE ID : CVE-2020-15415**	N/A	H-DRA-VIGO-070820/2037
easyrobotics					
er200					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-EAS-ER20-070820/2038
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given	https://github.com/aliasrobotics/RVD/issues/2565	H-EAS-ER20-070820/2039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-EAS-ER20-070820/2040
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by	https://github.com/aliasrobotics/RVD/issues/2562	H-EAS-ER20-070820/2041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**		
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	H-EAS-ER20-070820/2042
er-lite					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-EAS-ER-L-070820/2043
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with	https://github.com/aliasrobotics/RVD/issues/2565	H-EAS-ER-L-070820/2044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-EAS-ER-L-070820/2045
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine.	https://github.com/aliasrobotics/RVD/issues/2562	H-EAS-ER-L-070820/2046

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10277		
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	H-EAS-ER-L-070820/2047
er-flex					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-EAS-ER-F-070820/2048
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside	https://github.com/aliasrobotics/RVD/issues/2565	H-EAS-ER-F-070820/2049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-EAS-ER-F-070820/2050
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	H-EAS-ER-F-070820/2051
Improper	24-06-2020	5	The Apache server on port	https://gith	H-EAS-ER-F-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Shutdown or Release			80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	ub.com/aliasrobotics/RVD/issues/2568	070820/2052
er-one					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-EAS-ER-O-070820/2053
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and	https://github.com/aliasrobotics/RVD/issues/2565	H-EAS-ER-O-070820/2054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-EAS-ER-O-070820/2055
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	H-EAS-ER-O-070820/2056
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming	https://github.com/aliasrobotics/RVD/issues/	H-EAS-ER-O-070820/2057

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	2568	
enabled-robotics					
er-lite					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	H-ENA-ER-L-070820/2058
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This	https://github.com/aliasrobotics/RVD/issues/2557	H-ENA-ER-L-070820/2059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation	https://github.com/aliasrobotics/RVD/issues/2555	H-ENA-ER-L-070820/2060

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	H-ENA-ER-L-070820/2061
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed	https://github.com/aliasrobotics/RVD/issues/2560	H-ENA-ER-L-070820/2062

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			intellectual property and data. **CVE ID : CVE-2020-10273**		
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-ENA-ER-L-070820/2063
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	H-ENA-ER-L-070820/2064
er-flex					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default	https://github.com/aliasrobotics/RVD/issues/2566	H-ENA-ER-F-070820/2065

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw	https://github.com/aliasrobotics/RVD/issues/2557	H-ENA-ER-F-070820/2066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	https://github.com/aliasrobotics/RVD/issues/2555	H-ENA-ER-F-070820/2067
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph	https://github.com/aliasrobotics/RVD/issues/2554	H-ENA-ER-F-070820/2068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	H-ENA-ER-F-070820/2069
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-ENA-ER-F-070820/2070
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2	https://github.com/aliasrobotics/R	H-ENA-ER-F-070820/2071

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	VD/issues/ 2569	
er-one					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	H-ENA-ER-O-070820/2072
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet,	https://github.com/aliasrobotics/RVD/issues/	H-ENA-ER-O-070820/2073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**	2557	
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom	https://github.com/aliasrobotics/RVD/issues/2555	H-ENA-ER-O-070820/2074

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	H-ENA-ER-O-070820/2075
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the	https://github.com/aliasrobotics/RVD/issues/	H-ENA-ER-O-070820/2076

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	2560	
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-ENA-ER-O-070820/2077
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	H-ENA-ER-O-070820/2078
Honeywell					
controledge_plc					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes a session token on the network. **CVE ID : CVE-2020-10624**	N/A	H-HON-CONT-070820/2079
Cleartext Transmission of Sensitive Information	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes unencrypted passwords on the network. **CVE ID : CVE-2020-10628**	N/A	H-HON-CONT-070820/2080
controledge_rtu					
Cleartext Transmission of Sensitive Information	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes a session token on the network. **CVE ID : CVE-2020-10624**	N/A	H-HON-CONT-070820/2081
Cleartext Transmission of Sensitive Information	26-06-2020	5	ControlEdge PLC (R130.2, R140, R150, and R151) and RTU (R101, R110, R140, R150, and R151) exposes unencrypted passwords on the network. **CVE ID : CVE-2020-10628**	N/A	H-HON-CONT-070820/2082
Huawei					
p30_pro					
Improper Validation of Integrity Check Value	18-06-2020	2.1	HUAWEI P30 and HUAWEI P30 Pro with versions earlier than 10.1.0.135(C00E135R2P11) and versions earlier than 10.1.0.135(C00E135R2P8) have an insufficient integrity	N/A	H-HUA-P30_-070820/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check vulnerability. The system does not check certain software package's integrity sufficiently. Successful exploit could allow an attacker to load a crafted software package to the device. **CVE ID : CVE-2020-1834**		
p30					
Improper Validation of Integrity Check Value	18-06-2020	2.1	HUAWEI P30 and HUAWEI P30 Pro with versions earlier than 10.1.0.135(C00E135R2P11) and versions earlier than 10.1.0.135(C00E135R2P8) have an insufficient integrity check vulnerability. The system does not check certain software package's integrity sufficiently. Successful exploit could allow an attacker to load a crafted software package to the device. **CVE ID : CVE-2020-1834**	N/A	H-HUA-P30-070820/2084
mate_30					
Information Exposure	18-06-2020	3.3	HUAWEI Mate 30 with versions earlier than 10.1.0.126(C00E125R5P3) have an information disclosure vulnerability. A logic judgment error occurs when the system handling Bluetooth connections, an attacker could craft as an authenticated Bluetooth peer to launch the attack. Successful exploit could	N/A	H-HUA-MATE-070820/2085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause information disclosure. **CVE ID : CVE-2020-1835**		
Iball					
wrb303n					
Cross-Site Request Forgery (CSRF)	29-06-2020	4.3	iBall WRB303N devices allow CSRF attacks, as demonstrated by enabling remote management, enabling DHCP, or modifying the subnet range for IP addresses. **CVE ID : CVE-2020-15043**	N/A	H-IBA-WRB3-070820/2086
Intel					
82540em					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82540ep					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2088
82541ei					
Information	16-06-2020	5	Beckhoff's TwinCAT RT	https://cert	H-INT-8254-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	.vde.com/en-us/advisories/vde-2020-019	070820/2089
82541er					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82541gi					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2091

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82541pi					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests sent to the device. **CVE ID : CVE-2020-12494**		
82544ei					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2093
82544gc					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver	https://cert.vde.com/en-us/advisories/vde-	H-INT-8254-070820/2094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	2020-019	
82545em					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead,	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82545gm					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82546eb					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2097
82546gb					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2098
82547ei					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82547gi					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82547ei_					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8254-070820/2101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
82557					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8255-070820/2102
82558					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT	https://cert.vde.com/en-us/advisori	H-INT-8255-070820/2103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**	es/vde-2020-019	
82559					
Information Exposure	16-06-2020	5	Beckhoff's TwinCAT RT network driver for Intel 8254x and 8255x is providing EtherCAT functionality. The driver implements real-time features. Except for Ethernet frames sent from real-time functionality, all other Ethernet frames sent through the driver are not padded if their payload is less than the minimum	https://cert.vde.com/en-us/advisories/vde-2020-019	H-INT-8255-070820/2104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ethernet frame size. Instead, arbitrary memory content is transmitted within in the padding bytes of the frame. Most likely this memory contains slices from previously transmitted or received frames. By this method, memory content is disclosed, however, an attacker can hardly control which memory content is affected. For example, the disclosure can be provoked with small sized ICMP echo requests sent to the device. **CVE ID : CVE-2020-12494**		
kuka					
kr_c4					
N/A	16-06-2020	3.6	Critical services for operation can be terminated from windows task manager, bringing the manipulator to a halt. After this a Re-Calibration of the brakes needs to be performed. Be noted that this only can be accomplished either by a Kuka technician or by Kuka issued calibration hardware that interfaces with the manipulator furthering the delay and increasing operational costs. **CVE ID : CVE-2020-10268**	https://github.com/aliasrobotics/RVD/issues/2550	H-KUK-KR_C-070820/2105
maipu					
mp1800x-50					
Information	29-06-2020	5	The web interface of Maipu MP1800X-50 7.5.3.14(R)	N/A	H-MAI-MP18-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			devices allows remote attackers to obtain sensitive information via the form/formDeviceVerGet URI, such as system id, hardware model, hardware version, bootloader version, software version, software image file, compilation time, and system uptime. This is similar to CVE-2019-1653. **CVE ID : CVE-2020-13896**		070820/2106
mi					
mijia_inkjet_printer					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	7.5	An issue was discovered on Xiaomi Mi Jia ink-jet printer < 3.4.6_0138. Injecting parameters to ippserver through the web management background, resulting in command execution vulnerabilities. **CVE ID : CVE-2020-10561**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=13	H-MI-MIJI-070820/2107
xiaomi_r3600					
Information Exposure	24-06-2020	5	An unsafe configuration of nginx lead to information leak in Xiaomi router R3600 ROM before 1.0.50. **CVE ID : CVE-2020-11959**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=14	H-MI-XIAO-070820/2108
N/A	24-06-2020	7.5	Xiaomi router R3600 ROM before 1.0.50 is affected by a	https://privacy.mi.com/	H-MI-XIAO-070820/2109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability when checking backup file in c_upload interface let attacker able to extract malicious file under any location in /tmp, lead to possible RCE and DoS **CVE ID : CVE-2020-11960**	trust#/security/vulnerability-management/vulnerability-announcement/detail?id=15	
Information Exposure	24-06-2020	5	Xiaomi router R3600 ROM before 1.0.50 is affected by a sensitive information leakage caused by an insecure interface get_config_result without authentication **CVE ID : CVE-2020-11961**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=16	H-MI-XIAO-070820/2110
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	24-06-2020	7.5	In Xiaomi router R3600, ROM version<1.0.20, the connection service can be injected through the web interface, resulting in stack overflow or remote code execution. **CVE ID : CVE-2020-14094**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=17&locale=zh	H-MI-XIAO-070820/2111
Improper Neutralization of Special Elements in Output Used by a Downstream Component	24-06-2020	7.5	In Xiaomi router R3600, ROM version<1.0.20, a connect service suffers from an injection vulnerability through the web interface, leading to a stack overflow or remote code execution. **CVE ID : CVE-2020-14095**	https://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-	H-MI-XIAO-070820/2112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')				announcement/detail?id=18&locale=en	
Mitsubishielectric					
melsec_iq-r					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	H-MIT-MELS-070820/2113
melsec_iq-f					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	H-MIT-MELS-070820/2114
melsec-q					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3	N/A	H-MIT-MELS-070820/2115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**		
melsec-l					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	H-MIT-MELS-070820/2116
melsec-fx					
Cleartext Transmission of Sensitive Information	23-06-2020	7.5	Mitsubishi Electric MELSEC iQ-R, iQ-F, Q, L, and FX series CPU modules all versions contain a vulnerability that allows cleartext transmission of sensitive information between CPU modules and GX Works3 and/or GX Works2 via unspecified vectors. **CVE ID : CVE-2020-5594**	N/A	H-MIT-MELS-070820/2117
mobile-industrial-robotics					
er200					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default	https://github.com/aliasrobotics/RVD/issues/2566	H-MOB-ER20-070820/2118

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**		
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw	https://github.com/aliasrobotics/RVD/issues/2557	H-MOB-ER20-070820/2119

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**	https://github.com/aliasrobotics/RVD/issues/2555	H-MOB-ER20-070820/2120
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph	https://github.com/aliasrobotics/RVD/issues/2554	H-MOB-ER20-070820/2121

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**		
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and data. **CVE ID : CVE-2020-10273**	https://github.com/aliasrobotics/RVD/issues/2560	H-MOB-ER20-070820/2122
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-MOB-ER20-070820/2123
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2	https://github.com/aliasrobotics/R	H-MOB-ER20-070820/2124

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	VD/issues/2569	
mobile-industrial-robots					
mir100					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-MOB-MIR1-070820/2125
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given	https://github.com/aliasrobotics/RVD/issues/2565	H-MOB-MIR1-070820/2126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-MOB-MIR1-070820/2127
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by	https://github.com/aliasrobotics/RVD/issues/2562	H-MOB-MIR1-070820/2128

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**		
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	H-MOB-MIR1-070820/2129
mir200					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-MOB-MIR2-070820/2130
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with	https://github.com/aliasrobotics/RVD/issues/2565	H-MOB-MIR2-070820/2131

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-MOB-MIR2-070820/2132
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine.	https://github.com/aliasrobotics/RVD/issues/2562	H-MOB-MIR2-070820/2133

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10277		
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	H-MOB-MIR2-070820/2134
mir250					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-MOB-MIR2-070820/2135
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside	https://github.com/aliasrobotics/RVD/issues/2565	H-MOB-MIR2-070820/2136

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-MOB-MIR2-070820/2137
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	H-MOB-MIR2-070820/2138
Improper	24-06-2020	5	The Apache server on port	https://gith	H-MOB-MIR2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Shutdown or Release			80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	ub.com/aliasrobotics/RVD/issues/2568	070820/2139
mir500					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-MOB-MIR5-070820/2140
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and	https://github.com/aliasrobotics/RVD/issues/2565	H-MOB-MIR5-070820/2141

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-MOB-MIR5-070820/2142
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	H-MOB-MIR5-070820/2143
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming	https://github.com/aliasrobotics/RVD/issues/	H-MOB-MIR5-070820/2144

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	2568	
mir1000					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**	https://github.com/aliasrobotics/RVD/issues/2556	H-MOB-MIR1-070820/2145
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete	https://github.com/aliasrobotics/RVD/issues/2565	H-MOB-MIR1-070820/2146

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. **CVE ID : CVE-2020-10275**		
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**	https://github.com/aliasrobotics/RVD/issues/2558	H-MOB-MIR1-070820/2147
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	H-MOB-MIR1-070820/2148
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the	https://github.com/aliasrobotics/RVD/issues/2568	H-MOB-MIR1-070820/2149

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the dashboard. **CVE ID : CVE-2020-10280**		
Netapp					
hci_h610s					
Use of Hard-coded Credentials	29-06-2020	4	The NetApp HCI H610C, H615C and H610S Baseboard Management Controllers (BMC) are shipped with a documented default account and password that should be changed during the initial node setup. During upgrades to Element 11.8 and 12.0 or the Compute Firmware Bundle 12.2.92 the BMC account password on the H610C, H615C and H610S platforms is reset to the default documented value which could allow remote attackers to cause a Denial of Service (DoS). **CVE ID : CVE-2020-8573**	N/A	H-NET-HCI_-070820/2150
Netgear					
mk63					
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-	H-NET-MK63-070820/2151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	0050	
mr60					
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-MR60-070820/2152
ms60					
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-	H-NET-MS60-070820/2153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	on-Some-WiFi-Systems-PSV-2020-0050	
srk60					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	H-NET-SRK6-070820/2154
srk60b03					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-	H-NET-SRK6-070820/2155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	on-Some-WiFi-Systems-PSV-2020-0026	
srk60b04					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	H-NET-SRK6-070820/2156
srk60b05					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	H-NET-SRK6-070820/2157
srk60b06					
Improper	18-06-2020	5.8	Certain NETGEAR devices	https://kb.	H-NET-SRK6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	070820/2158
srr60					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before 2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0026	H-NET-SRR6-070820/2159
srs60					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects SRK60 before 2.5.2.104, SRS60 before 2.5.2.104, SRR60 before 2.5.2.104, SRK60B03 before 2.5.2.104, SRK60B04 before	https://kb.netgear.com/000061930/Security-Advisory-for-Pre-Authentication-Command-	H-NET-SRS6-070820/2160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.5.2.104, SRK60B05 before 2.5.2.104, and SRK60B06 before 2.5.2.104. **CVE ID : CVE-2020-14435**	Injection-on-Some-WiFi-Systems-PSV-2020-0026	
rbk752					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBK7-070820/2161
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25.	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	H-NET-RBK7-070820/2162

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14434		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBK7-070820/2163
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBK7-070820/2164
Improper Neutralization of Special	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/0000619	H-NET-RBK7-070820/2165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	41/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBK7-070820/2166
Improper Neutralization of Special Elements used in an OS Command ('OS	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authenticat	H-NET-RBK7-070820/2167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command Injection')			3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	ion-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBK7-070820/2168
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-	H-NET-RBK7-070820/2169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	0042	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBK7-070820/2170
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBK7-070820/2171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBK7-070820/2172
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBK7-070820/2173
Cross-Site Request	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This	https://kb.netgear.co	H-NET-RBK7-070820/2174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	m/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBK7-070820/2175
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-	H-NET-RBK7-070820/2176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	
rbk753					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBK7-070820/2177
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-	H-NET-RBK7-070820/2178

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	Systems-PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBK7-070820/2179
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBK7-070820/2180

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14437		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBK7-070820/2181
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBK7-070820/2182
Improper Neutralization of Special	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/0000619	H-NET-RBK7-070820/2183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	43/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBK7-070820/2184
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-	H-NET-RBK7-070820/2185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	on-Some-WiFi-Systems-PSV-2020-0042	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBK7-070820/2186
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBK7-070820/2187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBK7-070820/2188
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBK7-070820/2189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14431		
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBK7-070820/2190
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBK7-070820/2191
Improper Neutralization of Special Elements used in an OS	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before	https://kb.netgear.com/000061947/Security-Advisory-	H-NET-RBK7-070820/2192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	
rbk753s					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBK7-070820/2193
Improper Neutralization of Special Elements in Output Used by a Downstream Component	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-	H-NET-RBK7-070820/2194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	Injection-on-Some-WiFi-Systems-PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBK7-070820/2195
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-	H-NET-RBK7-070820/2196

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBK7-070820/2197
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBK7-070820/2198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14439		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	H-NET-RBK7-070820/2199
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBK7-070820/2200
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before	https://kb.netgear.com/000061935/Security	H-NET-RBK7-070820/2201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBK7-070820/2202
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-	H-NET-RBK7-070820/2203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	Systems-PSV-2020-0050	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBK7-070820/2204
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-	H-NET-RBK7-070820/2205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBK7-070820/2206
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBK7-070820/2207

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	H-NET-RBK7-070820/2208
rbr750					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBR7-070820/2209
Improper Neutralization of Special Elements in	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752	https://kb.netgear.com/000061934/Security	H-NET-RBR7-070820/2210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Output Used by a Downstream Component ('Injection')			before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBR7-070820/2211
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-	H-NET-RBR7-070820/2212

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	Injection-on-Some-WiFi-Systems-PSV-2020-0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBR7-070820/2213
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	H-NET-RBR7-070820/2214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	H-NET-RBR7-070820/2215
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11.	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBR7-070820/2216

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14426		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	H-NET-RBR7-070820/2217
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBR7-070820/2218
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before	https://kb.netgear.com/000061938/Security-Advisory-	H-NET-RBR7-070820/2219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBR7-070820/2220
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-	H-NET-RBR7-070820/2221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBR7-070820/2222
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-	H-NET-RBR7-070820/2223

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	H-NET-RBR7-070820/2224
rbs750					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25.	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBS7-070820/2225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14433		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	H-NET-RBS7-070820/2226
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBS7-070820/2227
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061940/Security	H-NET-RBS7-070820/2228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBS7-070820/2229
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-	H-NET-RBS7-070820/2230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	H-NET-RBS7-070820/2231
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-	H-NET-RBS7-070820/2232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	H-NET-RBS7-070820/2233
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBS7-070820/2234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBS7-070820/2235
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBS7-070820/2236
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of	https://kb.netgear.co	H-NET-RBS7-070820/2237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	m/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBS7-070820/2238
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-	H-NET-RBS7-070820/2239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	Injection-on-Some-WiFi-Systems-PSV-2020-0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	H-NET-RBS7-070820/2240
rbk852					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-	H-NET-RBK8-070820/2241

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	H-NET-RBK8-070820/2242
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25.	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBK8-070820/2243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14436		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBK8-070820/2244
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBK8-070820/2245
Improper Neutralization of Special	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/0000619	H-NET-RBK8-070820/2246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	42/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	H-NET-RBK8-070820/2247
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-	H-NET-RBK8-070820/2248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	H-NET-RBK8-070820/2249
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBK8-070820/2250

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**		
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBK8-070820/2251
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBK8-070820/2252

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25. **CVE ID : CVE-2020-14430**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBK8-070820/2253
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBK8-070820/2254
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061946/Security	H-NET-RBK8-070820/2255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	H-NET-RBK8-070820/2256
rbk853					
Improper Neutralization of Special Elements in Output Used by a Downstream	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authenticat	H-NET-RBK8-070820/2257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	ion-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	H-NET-RBK8-070820/2258
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	H-NET-RBK8-070820/2259

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	PSV-2020-0039	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBK8-070820/2260
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBK8-070820/2261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14438		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBK8-070820/2262
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	H-NET-RBK8-070820/2263
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials.	https://kb.netgear.com/0000619	H-NET-RBK8-070820/2264

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	31/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	H-NET-RBK8-070820/2265
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-	H-NET-RBK8-070820/2266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	WiFi-Systems-PSV-2020-0044	
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBK8-070820/2267
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-	H-NET-RBK8-070820/2268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	PSV-2020-0051	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBK8-070820/2269
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBK8-070820/2270

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBK8-070820/2271
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	H-NET-RBK8-070820/2272
rbr850					
Improper Neutralization of Special	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated	https://kb.netgear.com/0000619	H-NET-RBR8-070820/2273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	32/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	H-NET-RBR8-070820/2274
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-	H-NET-RBR8-070820/2275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	Injection-on-Some-WiFi-Systems-PSV-2020-0039	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBR8-070820/2276
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	H-NET-RBR8-070820/2277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	PSV-2020-0063	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBR8-070820/2278
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	H-NET-RBR8-070820/2279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14440		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBR8-070820/2280
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	H-NET-RBR8-070820/2281
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before	https://kb.netgear.com/000061936/Security-Advisory-	H-NET-RBR8-070820/2282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBR8-070820/2283
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-	H-NET-RBR8-070820/2284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBR8-070820/2285
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBR8-070820/2286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBR8-070820/2287
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	H-NET-RBR8-070820/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rbs850					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBS8-070820/2289
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	H-NET-RBS8-070820/2290
Improper Neutralization of Special Elements in Output Used	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before	https://kb.netgear.com/000061933/Security-Advisory-	H-NET-RBS8-070820/2291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
by a Downstream Component ('Injection')			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBS8-070820/2292
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-	H-NET-RBS8-070820/2293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	Injection-on-Some-WiFi-Systems-PSV-2020-0063	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBS8-070820/2294
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-	H-NET-RBS8-070820/2295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBS8-070820/2296
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	H-NET-RBS8-070820/2297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBS8-070820/2298
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBS8-070820/2299
Insufficiently Protected	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of	https://kb.netgear.co	H-NET-RBS8-070820/2300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	m/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBS8-070820/2301
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-	H-NET-RBS8-070820/2302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	Forgery-on-Some-WiFi-Systems-PSV-2020-0049	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBS8-070820/2303
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-	H-NET-RBS8-070820/2304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	0103	
rbk842					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBK8-070820/2305
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0040	H-NET-RBK8-070820/2306

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBK8-070820/2307
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBK8-070820/2308
Improper Neutralization of Special Elements	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker.	https://kb.netgear.com/000061941/Security	H-NET-RBK8-070820/2309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBK8-070820/2310
Improper Neutralization of Special Elements used in an OS Command ('OS Command	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-	H-NET-RBK8-070820/2311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBK8-070820/2312
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	H-NET-RBK8-070820/2313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBK8-070820/2314
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBK8-070820/2315

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25. **CVE ID : CVE-2020-14429**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBK8-070820/2316
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBK8-070820/2317
Cross-Site Request Forgery	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before	https://kb.netgear.com/0000619	H-NET-RBK8-070820/2318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	37/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBK8-070820/2319
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-	H-NET-RBK8-070820/2320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	Injection-on-Some-WiFi-Systems-PSV-2020-0103	
rbr840					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBR8-070820/2321
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-	H-NET-RBR8-070820/2322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBR8-070820/2323
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0054	H-NET-RBR8-070820/2324

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14437		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBR8-070820/2325
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14439**	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBR8-070820/2326
Improper Neutralization of Special	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an	https://kb.netgear.com/0000619	H-NET-RBR8-070820/2327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	43/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBR8-070820/2328
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before	https://kb.netgear.com/000061935/Security-Advisory-for-Admin-Credential-Disclosure-	H-NET-RBR8-070820/2329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	on-Some-WiFi-Systems-PSV-2020-0042	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBR8-070820/2330
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-RBR8-070820/2331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**		
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBR8-070820/2332
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0068	H-NET-RBR8-070820/2333

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14431		
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBR8-070820/2334
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBR8-070820/2335
Improper Neutralization of Special Elements used in an OS	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before	https://kb.netgear.com/000061947/Security-Advisory-	H-NET-RBR8-070820/2336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	
rbs840					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.2	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBK842 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, and RBS750 before 3.2.15.25. **CVE ID : CVE-2020-14433**	https://kb.netgear.com/000061932/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0035	H-NET-RBS8-070820/2337
Improper Neutralization of Special Elements in Output Used by a Downstream Component	18-06-2020	7.7	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852	https://kb.netgear.com/000061934/Security-Advisory-for-Post-Authentication-Command-	H-NET-RBS8-070820/2338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14434**	Injection-on-Some-WiFi-Systems-PSV-2020-0040	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, RBS850 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, and RBS840 before 3.2.15.25. **CVE ID : CVE-2020-14436**	https://kb.netgear.com/000061933/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0039	H-NET-RBS8-070820/2339
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before	https://kb.netgear.com/000061940/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-	H-NET-RBS8-070820/2340

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14437**	0054	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14438**	https://kb.netgear.com/000061941/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0063	H-NET-RBS8-070820/2341
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25.	https://kb.netgear.com/000061942/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0064	H-NET-RBS8-070820/2342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14439		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14440**	https://kb.netgear.com/000061943/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0065	H-NET-RBS8-070820/2343
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK852 before 3.2.10.11, RBK853 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, RBK842 before 3.2.10.11, RBR840 before 3.2.10.11, and RBS840 before 3.2.10.11. **CVE ID : CVE-2020-14426**	https://kb.netgear.com/000061931/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-Wifi-Systems-PSV-2020-0033	H-NET-RBS8-070820/2344
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before	https://kb.netgear.com/000061935/Security	H-NET-RBS8-070820/2345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14427**	-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0042	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14428**	https://kb.netgear.com/000061936/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0044	H-NET-RBS8-070820/2346
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-	H-NET-RBS8-070820/2347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	Systems-PSV-2020-0050	
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14430**	https://kb.netgear.com/000061939/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0051	H-NET-RBS8-070820/2348
Insufficiently Protected Credentials	18-06-2020	3.3	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before	https://kb.netgear.com/000061944/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-	H-NET-RBS8-070820/2349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14431**	0068	
Cross-Site Request Forgery (CSRF)	18-06-2020	6.8	Certain NETGEAR devices are affected by CSRF. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14432**	https://kb.netgear.com/000061937/Security-Advisory-for-Cross-Site-Request-Forgery-on-Some-WiFi-Systems-PSV-2020-0049	H-NET-RBS8-070820/2350
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14441**	https://kb.netgear.com/000061946/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0071	H-NET-RBS8-070820/2351

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	18-06-2020	5.8	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBR750 before 3.2.15.25, RBS750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14442**	https://kb.netgear.com/000061947/Security-Advisory-for-Pre-Authentication-Command-Injection-on-Some-WiFi-Systems-PSV-2020-0103	H-NET-RBS8-070820/2352
mk62					
Insufficiently Protected Credentials	18-06-2020	5.8	Certain NETGEAR devices are affected by disclosure of administrative credentials. This affects MK62 before 1.0.4.92, MK63 before 1.0.4.92, MR60 before 1.0.4.92, MS60 before 1.0.4.92, RBK752 before 3.2.15.25, RBK753 before 3.2.15.25, RBK753S before 3.2.15.25, RBS750 before 3.2.15.25, RBR750 before 3.2.15.25, RBK842 before 3.2.15.25, RBR840 before 3.2.15.25, RBS840 before 3.2.15.25, RBK852 before 3.2.15.25, RBK853 before 3.2.15.25, RBR850 before 3.2.15.25, and RBS850 before 3.2.15.25. **CVE ID : CVE-2020-14429**	https://kb.netgear.com/000061938/Security-Advisory-for-Admin-Credential-Disclosure-on-Some-WiFi-Systems-PSV-2020-0050	H-NET-MK62-070820/2353

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Nvidia					
quadro					
Improper Privilege Management	24-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-QUAD-070820/2354
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-QUAD-070820/2355
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	H-NVI-QUAD-070820/2356
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode	https://nvidia.custhelp.com/app/answers/det	H-NVI-QUAD-070820/2357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to denial of service. **CVE ID : CVE-2020-5965**	ail/a_id/5031	
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-QUAD-070820/2358
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-QUAD-070820/2359
tesla					
Improper Privilege Management	24-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-TESL-070820/2360

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-TESL-070820/2361
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	H-NVI-TESL-070820/2362
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to denial of service. **CVE ID : CVE-2020-5965**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-TESL-070820/2363
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-TESL-070820/2364

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**		
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-TESL-070820/2365
geforce					
Improper Privilege Management	24-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-GEFO-070820/2366
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-GEFO-070820/2367
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application	https://nvidia.custhelp.com/app/answers/detail/a_id/50	H-NVI-GEFO-070820/2368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	31, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to denial of service. **CVE ID : CVE-2020-5965**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-GEFO-070820/2369
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-GEFO-070820/2370
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-GEFO-070820/2371
nvs					
Improper	24-06-2020	4.6	NVIDIA Windows GPU	https://nvi	H-NVI-NVS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Privilege Management			Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component, in which an attacker with local system access can corrupt a system file, which may lead to denial of service or escalation of privileges. **CVE ID : CVE-2020-5962**	dia.custhelp.com/app/answers/detail/a_id/5031	070820/2372
Improper Privilege Management	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure. **CVE ID : CVE-2020-5963**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-NVS-070820/2373
Improper Validation of Integrity Check Value	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the service host component, in which the application resources integrity check may be missed. Such an attack may lead to code execution, denial of service or information disclosure. **CVE ID : CVE-2020-5964**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031, https://nvidia.custhelp.com/app/answers/detail/a_id/5038	H-NVI-NVS-070820/2374
Out-of-bounds Read	25-06-2020	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX 11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, leading to	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-NVS-070820/2375

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service. **CVE ID : CVE-2020-5965**		
NULL Pointer Dereference	25-06-2020	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape, in which a NULL pointer is dereferenced, leading to denial of service or potential escalation of privileges. **CVE ID : CVE-2020-5966**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-NVS-070820/2376
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	25-06-2020	1.9	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service. **CVE ID : CVE-2020-5967**	https://nvidia.custhelp.com/app/answers/detail/a_id/5031	H-NVI-NVS-070820/2377
Philips					
clearvue_850					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information.	N/A	H-PHI-CLEA-070820/2378

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14477		
clearvue_350					
Improper Authenticati on	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	H-PHI-CLEA-070820/2379
cx50					
Improper Authenticati on	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	H-PHI-CX50-070820/2380
affiniti_70					
Improper Authenticati	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX	N/A	H-PHI-AFFI-070820/2381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**		
affiniti_50					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	H-PHI-AFFI-070820/2382
epiq_7					
Improper Authentication	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and	N/A	H-PHI-EPIQ-070820/2383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**		
sparq					
Improper Authenticati on	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the alternate service login to view or modify information. **CVE ID : CVE-2020-14477**	N/A	H-PHI-SPAR-070820/2384
xperius					
Improper Authenticati on	26-06-2020	3.6	In Philips Ultrasound ClearVue Versions 3.2 and prior, Ultrasound CX Versions 5.0.2 and prior, Ultrasound EPIQ/Affiniti Versions VM5.0 and prior, Ultrasound Sparq Version 3.0.2 and prior and Ultrasound Xperius all versions, an attacker may use an alternate path or channel that does not require authentication of the	N/A	H-PHI-XPER-070820/2385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			alternate service login to view or modify information. **CVE ID : CVE-2020-14477**		
Qualcomm					
mdm9206					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2386

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2387
Improper	22-06-2020	7.5	Possible null-pointer	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	MDM9-070820/2388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2389

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2391
mdm9607					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2392

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3614		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2393
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-MDM9-070820/2394

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2397
msm8909w					
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-070820/2398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	lletins/june-2020-bulletin	
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2401
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table	https://www.qualcomm.com/company/produ	H-QUA-MSM8-070820/2402

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	ct-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2403

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2405
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the	https://www.qualcomm.com/company/produ	H-QUA-MSM8-070820/2406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	ct-security/bulletins/june-2020-bulletin	
msm8996au					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2408

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2409
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2410

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2411

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2412

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2413
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2415

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
qca6574au					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2416

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2417

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3626		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2418
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-QCA6-070820/2419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2422
qcs405					
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCS4-070820/2423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table	https://www.qualcomm.com/company/produ	H-QUA-QCS4-070820/2424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	ct-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS4-070820/2425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS4-070820/2426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS4-070820/2427
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size	https://www.qualcomm.com/company/produ	H-QUA-QCS4-070820/2428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	ct-security/bulletins/june-2020-bulletin	
qcs605					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2431

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2432
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2433

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2434
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in	https://www.qualcomm.com/company/product-security/bu	H-QUA-QCS6-070820/2435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	lletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCS6-070820/2438
sda660					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDA6-070820/2439

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDA6-070820/2440

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDA6-070820/2441
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-SDA6-070820/2442

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDA6-070820/2443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDA6-070820/2444

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
sdm439					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2446
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2447

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2448

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2449
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds	https://www.qualcomm.com/company/produ	H-QUA-SDM4-070820/2450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	ct-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2452

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2453
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDM4-070820/2454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	lletins/june-2020-bulletin	
sdm630					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2455

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2456

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2457
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2458

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2459

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2460

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3661		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2461
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2463

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3676		
sdm660					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2464

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2465
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2467

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2468
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-SDM6-070820/2469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2471

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2472
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sdx20					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2474

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Privilege Management	22-06-2020	10	Improper access due to socket opened by the logging application without specifying localhost address in Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, Rennell, SDX20 **CVE ID : CVE-2020-3628**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2475
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2476

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2477

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2478
Buffer Copy without	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header	https://www.qualcom	H-QUA-SDX2-070820/2479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	m.com/company/product-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
mdm9640					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2483
mdm9650					
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-MDM9-070820/2484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range	https://www.qualcomm.com/company/product-security/bu	H-QUA-MDM9-070820/2485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	lletins/june-2020-bulletin	
sdx24					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDX2-070820/2487

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
ipq8074					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-IPQ8-070820/2488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
qca6174a					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA6-070820/2490

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
qca9377					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA9-070820/2491

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCA9-070820/2492
qca9379					
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-QCA9-070820/2493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range	https://www.qualcomm.com/company/product-security/bu	H-QUA-QCA9-070820/2494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	lletins/june-2020-bulletin	
sdm429w					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2496

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2497
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-SDM4-070820/2498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2500

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2501
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-SDM4-070820/2502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	-2020-bulletin	
sc7180					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SC71-070820/2503

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
apq8009					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2507

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2508
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**		
apq8098					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2512
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds	https://www.qualcomm.com/company/produ	H-QUA-APQ8-070820/2513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2514

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2515

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3660		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2516
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-APQ8-070820/2517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2518

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2519
msm8953					
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	security/bulletins/june-2020-bulletin	
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon	https://www.qualcomm.com/company/produ	H-QUA-MSM8-070820/2521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2523
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with	https://www.qualcomm.com/com	H-QUA-MSM8-070820/2524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	pany/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2525

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2526

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2527
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array	https://www.qualcomm.com/com	H-QUA-MSM8-070820/2528

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	pany/product-security/bulletins/june-2020-bulletin	
msm8998					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2531
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2532

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2533

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2535
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2537

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
nicobar					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-NICO-070820/2538

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-NICO-070820/2539
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-NICO-070820/2540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-NICO-070820/2541
apq8053					
Buffer Copy without Checking	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of	https://www.qualcomm.com/com	H-QUA-APQ8-070820/2542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	pany/product-security/bulletins/june-2020-bulletin	
Incorrect Default	22-06-2020	4.6	Any application can bind to it and exercise the APIs due	https://www.qualcom	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/2543
Improper Privilege Management	22-06-2020	10	Improper access due to socket opened by the logging application without specifying localhost address in Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, Rennell, SDX20 **CVE ID : CVE-2020-3628**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2544
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-APQ8-070820/2545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2546

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2547
Buffer Copy without Checking	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms	https://www.qualcomm.com/com	H-QUA-APQ8-070820/2548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	pany/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2549

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2551
mdm9207c					
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before	https://www.qualcomm.com/company/produ	H-QUA-MDM9-070820/2552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with	https://www.qualcomm.com/com	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	pany/product-security/bulletins/june-2020-bulletin	070820/2553
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2554

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2557
msm8905					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-MSM8-070820/2559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2560

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2561
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds	https://www.qualcomm.com/company/produ	H-QUA-MSM8-070820/2562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
sdm845					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM8-070820/2564

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM8-070820/2565

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM8-070820/2566
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-SDM8-070820/2567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM8-070820/2568
Improper	22-06-2020	7.5	Possible null-pointer	https://ww	H-QUA-SDM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation of Array Index			dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	w.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	070820/2569
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM8-070820/2570

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM8-070820/2571

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM8-070820/2572
apq8076					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2573

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3614		
apq8017					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2575
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-APQ8-070820/2576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2578

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2579
apq8096au					
Buffer Copy without Checking Size of Input	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before	https://www.qualcomm.com/company/produ	H-QUA-APQ8-070820/2580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	ct-security/bulletins/june-2020-bulletin	
Incorrect Default	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL	https://www.qualcomm.com/com	H-QUA-APQ8-070820/2581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permissions			uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	pany/product-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2582

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2583
Improper Validation of	22-06-2020	7.5	Possible null-pointer dereference can occur while	https://www.qualcom	H-QUA-APQ8-070820/2584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	m.com/company/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2585

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2587
Improper Validation of	22-06-2020	4.6	A possible buffer overflow would occur while	https://www.qualcom	H-QUA-APQ8-070820/2588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Array Index			processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	m.com/company/product-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2589

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sdm636					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2591
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-SDM6-070820/2592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2593

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2594
Buffer Copy without	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with	https://www.qualcom	H-QUA-SDM6-070820/2595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	m.com/company/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-SDM6-070820/2596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2597

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2598
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user	https://www.qualcomm.com/company/produ	H-QUA-SDM6-070820/2599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	ct-security/bulletins/june-2020-bulletin	
sdm670					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2600

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2601

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2602
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2603

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2604
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to	https://www.qualcomm.com/company/product-	H-QUA-SDM6-070820/2605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2606

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2607

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3676		
sdm710					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2608

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2609
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2611
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2612

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2613

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2614

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM7-070820/2615
sxr1130					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR1-070820/2616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR1-070820/2617

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR1-070820/2618
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer	https://www.qualcomm.com/company/produ	H-QUA-SXR1-070820/2619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR1-070820/2620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3658**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR1-070820/2621
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size	https://www.qualcomm.com/company/produ	H-QUA-SXR1-070820/2622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	ct-security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR1-070820/2623

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sm6150					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM61-070820/2624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM61-070820/2625
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds	https://www.qualcomm.com/company/produ	H-QUA-SM61-070820/2626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	ct-security/bulletins/june-2020-bulletin	
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM61-070820/2627
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SM61-070820/2628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM61-070820/2629

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM61-070820/2630

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM61-070820/2631
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SM61-070820/2632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM61-070820/2633

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sm8150					
Double Free	22-06-2020	7.2	Double free issue in kernel memory mapping due to lack of memory protection mechanism in Snapdragon Compute, Snapdragon Mobile, Snapdragon Voice & Music in SM8150 **CVE ID : CVE-2020-3613**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2634
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2637
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2638

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3642**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2639
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SM81-070820/2640

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	lletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2642

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2643
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range	https://www.qualcomm.com/company/product-security/bu	H-QUA-SM81-070820/2644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	lletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM81-070820/2645

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
mdm9615					
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MDM9-070820/2646
msm8909					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-MSM8-070820/2647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	bulletin	
qca6584au					
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-QCA6-070820/2648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	security/bulletins/june-2020-bulletin	
qca9886					
Buffer Copy without	22-06-2020	7.5	Possible buffer overflow while copying the frame to	https://www.qualcom	H-QUA-QCA9-070820/2649

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	m.com/company/product-security/bulletins/june-2020-bulletin	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qm215					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2650

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2651
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2652

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2653

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2654
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-QM21-070820/2655

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2656

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2657

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QM21-070820/2658
sm7150					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2659

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2660

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2661
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer	https://www.qualcomm.com/company/produ	H-QUA-SM71-070820/2662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2664
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2665

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2666

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2667

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM71-070820/2668
sdm429					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2669

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2671
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SDM4-070820/2672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2673

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2674

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2675
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SDM4-070820/2676

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	security/bulletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2677

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sdm632					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2679
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-SDM6-070820/2680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2682

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2683
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-SDM6-070820/2684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2685

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM6-070820/2686
msm8917					
Buffer Copy without Checking Size of Input ('Classic Buffer	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-MSM8-070820/2687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	-2020-bulletin	
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bu	H-QUA-MSM8-070820/2688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	lletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2690
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2692

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2693

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2694
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	security/bulletins/june-2020-bulletin	
msm8920					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2698
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2701

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2702
msm8937					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2703

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2704

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2705
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with	https://www.qualcomm.com/com	H-QUA-MSM8-070820/2706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	pany/product-security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2707

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2709
msm8940					
Buffer Copy without Checking Size of Input ('Classic	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**	security/bulletins/june-2020-bulletin	
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon	https://www.qualcomm.com/company/produ	H-QUA-MSM8-070820/2711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	ct-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2713
Buffer Copy without Checking	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms	https://www.qualcomm.com/com	H-QUA-MSM8-070820/2714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	pany/product-security/bulletins/june-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2716

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
msm8996					
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2717
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto,	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	security/bulletins/june-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2719

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2720

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-MSM8-070820/2721
Improper Validation of Array Index	22-06-2020	4.6	A possible buffer overflow would occur while processing command from firmware due to the group_id obtained from the	https://www.qualcomm.com/company/product-	H-QUA-MSM8-070820/2722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			firmware being out of range in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9615, MDM9640, MDM9650, MSM8909W, MSM8996, MSM8996AU, QCA6174A, QCA9377, QCA9379, SDM439, SDM636, SDM660, SDX20, SDX24, SM8150 **CVE ID : CVE-2020-3665**	security/bulletins/june-2020-bulletin	
sdm450					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2724

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2725
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDM4-070820/2726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	lletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2728

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2729
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bu	H-QUA-SDM4-070820/2730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**	lletins/june-2020-bulletin	
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SDM4-070820/2731

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sm8250					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2732
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-SM82-070820/2733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	bulletin	
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2734
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2735

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2736

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2737

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2738
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SM82-070820/2740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sxr2130					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2741
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**		
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2743
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2747
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SXR2-070820/2749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3676**		
sc8180x					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SC81-070820/2750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
qcm2150					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCM2-070820/2751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-QCM2-070820/2752
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-QCM2-070820/2753

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	-2020-bulletin	
apq8096					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-APQ8-070820/2754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
rennell					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Improper Privilege Management	22-06-2020	10	Improper access due to socket opened by the logging application without specifying localhost address in Snapdragon Consumer IOT, Snapdragon Mobile in APQ8053, Rennell, SDX20 **CVE ID : CVE-2020-3628**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2757
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2758
Use After	22-06-2020	4.6	Use after free issue in camera applications when	https://www.qualcom	H-QUA-RENN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	m.com/company/product-security/bulletins/june-2020-bulletin	070820/2759
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2760

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2761
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-	H-QUA-RENN-070820/2762

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2764

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-RENN-070820/2765
saipan					
Incorrect Default Permissions	22-06-2020	4.6	Any application can bind to it and exercise the APIs due to no protection for AIDL uimlpaservice in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2766

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA6574AU, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3626**		
Out-of-bounds Write	22-06-2020	4.6	Stack based overflow If the maximum number of arguments allowed per request in perflock exceeds in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables in APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3635**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2767
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after	https://www.qualcomm.com/company/product-	H-QUA-SAIP-070820/2768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3642**	security/bulletins/june-2020-bulletin	
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2769

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3658		
Improper Validation of Array Index	22-06-2020	7.5	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3660**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2770
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow can occur while parsing eac3 header while playing the clip which is nonstandard in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MSM8909W, MSM8917, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3662**		
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2773

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-SAIP-070820/2774
ipq6018					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Possible buffer overflow while copying the frame to local buffer due to lack of check of length before copying in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-IPQ6-070820/2775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking in APQ8009, APQ8017, APQ8053, APQ8076, APQ8096, APQ8096AU, APQ8098, IPQ6018, IPQ8074, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, MSM8998, Nicobar, QCA6174A, QCA6574AU, QCA6584AU, QCA9377, QCA9379, QCA9886, QCM2150, QCS405, QCS605, QM215, Rennell, SC7180, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SDX24, SM6150, SM7150, SM8150, SXR1130 **CVE ID : CVE-2020-3614**		
kamorta					
Use After Free	22-06-2020	4.6	Use after free issue in camera applications when used randomly over multiple operations due to pointer not set to NULL after free/destroy of the object in Snapdragon Consumer IOT, Snapdragon Mobile in Kamorta, QCS605, Rennell, Saipan, SDM670, SDM710, SDM845, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-KAMO-070820/2776

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3642		
Out-of-bounds Read	22-06-2020	6.4	Possible null-pointer dereference can occur while parsing mp4 clip with corrupted sample table atoms in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3658**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-KAMO-070820/2777
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-06-2020	7.5	Buffer overflow will happen while parsing mp4 clip with corrupted sample atoms values which exceeds MAX_UINT32 range due to lack of validation checks in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/june	H-QUA-KAMO-070820/2778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3661**	-2020-bulletin	
Out-of-bounds Write	22-06-2020	7.5	Buffer over-write may occur during fetching track decoder specific information if cb size exceeds buffer size in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-KAMO-070820/2779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, QCA6574AU, QCS405, QCS605, QM215, Rennell, Saipan, SDA660, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3663**		
Improper Validation of Array Index	22-06-2020	4.6	Possible memory corruption in perfservice due to improper validation array length taken from user application. in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile in APQ8096AU, APQ8098, Kamorta, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8998, Nicobar, QCM2150, QCS605, QM215, Rennell, Saipan, SDM429, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3676**	https://www.qualcomm.com/company/product-security/bulletins/june-2020-bulletin	H-QUA-KAMO-070820/2780
satoshilabs					

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
trezor_model_t					
Improper Verification of Cryptographic Signature	16-06-2020	4.3	BIP-143 in the Bitcoin protocol specification mishandles the signing of a Segwit transaction, which allows attackers to trick a user into making two signatures in certain cases, potentially leading to a huge transaction fee. NOTE: this affects all hardware wallets. It was fixed in 1.9.1 for the Trezor One and 2.3.1 for the Trezor Model T. **CVE ID : CVE-2020-14199**	N/A	H-SAT-TREZ-070820/2781
trezor_one					
Improper Verification of Cryptographic Signature	16-06-2020	4.3	BIP-143 in the Bitcoin protocol specification mishandles the signing of a Segwit transaction, which allows attackers to trick a user into making two signatures in certain cases, potentially leading to a huge transaction fee. NOTE: this affects all hardware wallets. It was fixed in 1.9.1 for the Trezor One and 2.3.1 for the Trezor Model T. **CVE ID : CVE-2020-14199**	N/A	H-SAT-TREZ-070820/2782
Schneider-electric					
easergy_t300					
Cross-Site Request Forgery (CSRF)	16-06-2020	6.8	A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to execute malicious	N/A	H-SCH-EASE-070820/2783

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands on behalf of a legitimate user when xsrf-token data is intercepted. **CVE ID : CVE-2020-7503**		
Improper Input Validation	16-06-2020	5	A CWE-20: Improper Input Validation vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to disable the webserver service on the device when specially crafted network packets are sent. **CVE ID : CVE-2020-7504**	N/A	H-SCH-EASE-070820/2784
Download of Code Without Integrity Check	16-06-2020	9	A CWE-494 Download of Code Without Integrity Check vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to inject data with dangerous content into the firmware and execute arbitrary code on the system. **CVE ID : CVE-2020-7505**	N/A	H-SCH-EASE-070820/2785
Information Exposure	16-06-2020	5	A CWE-538: File and Directory Information Exposure vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to pack or unpack the archive with the firmware for the controller and modules using the usual tar archiver resulting in an information exposure.	N/A	H-SCH-EASE-070820/2786

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7506		
Uncontrolled Resource Consumption	16-06-2020	5	A CWE-400: Uncontrolled Resource Consumption vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to login multiple times resulting in a denial of service. **CVE ID : CVE-2020-7507**	N/A	H-SCH-EASE-070820/2787
Improper Restriction of Excessive Authenticati on Attempts	16-06-2020	5	A CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to gain full access by brute force. **CVE ID : CVE-2020-7508**	N/A	H-SCH-EASE-070820/2788
Improper Privilege Management	16-06-2020	6.5	A CWE-269: Improper privilege management (write) vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to elevate their privileges and delete files. **CVE ID : CVE-2020-7509**	N/A	H-SCH-EASE-070820/2789
N/A	16-06-2020	7.5	A CWE-1103: Use of Platform-Dependent Third Party Components with vulnerabilities vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to exploit the component.	N/A	H-SCH-EASE-070820/2790

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7512		
Cleartext Storage of Sensitive Information	16-06-2020	5	A CWE-312: Cleartext Storage of Sensitive Information vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to intercept traffic and read configuration data. **CVE ID : CVE-2020-7513**	N/A	H-SCH-EASE-070820/2791
se					
modicon_m218					
Out-of-bounds Write	16-06-2020	5	A CWE-787: Out-of-bounds Write vulnerability exists in Modicon M218 Logic Controller (Firmware version 4.3 and prior), which may cause a Denial of Service when specific TCP/IP crafted packets are sent to the Modicon M218 Logic Controller. **CVE ID : CVE-2020-7502**	N/A	H-SE-MODI-070820/2792
easergy_t300					
Information Exposure	16-06-2020	5	A CWE-200: Information Exposure vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow attacker to obtain private keys. **CVE ID : CVE-2020-7510**	N/A	H-SE-EASE-070820/2793
Use of a Broken or Risky Cryptographic Algorithm	16-06-2020	5	A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists in Easergy T300 (Firmware version 1.5.2 and older) which could allow an attacker to acquire a	N/A	H-SE-EASE-070820/2794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password by brute force. **CVE ID : CVE-2020-7511**		
mtn6501-0001					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	H-SE-MTN6-070820/2795
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	H-SE-MTN6-070820/2796
mtn6501-0002					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes.	N/A	H-SE-MTN6-070820/2797

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7499		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	H-SE-MTN6-070820/2798
mtn6260-0410					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	H-SE-MTN6-070820/2799
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	H-SE-MTN6-070820/2800

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mtn6260-0415					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	H-SE-MTN6-070820/2801
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	H-SE-MTN6-070820/2802
mtn6260-0310					
Incorrect Authorization	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	H-SE-MTN6-070820/2803
Improper Neutralizatio	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special	N/A	H-SE-MTN6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an SQL Command ('SQL Injection')			Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**		070820/2804
mtn6260-0315					
Incorrect Authorizatio n	16-06-2020	4	A CWE-284:Improper Access Control vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause unauthorized access when a low privileged user makes unauthorized changes. **CVE ID : CVE-2020-7499**	N/A	H-SE-MTN6-070820/2805
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	16-06-2020	7.5	A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists in U.motion Servers and Touch Panels (affected versions listed in the security notification) which could cause arbitrary code to be executed when a malicious command is entered. **CVE ID : CVE-2020-7500**	N/A	H-SE-MTN6-070820/2806
Sophos					
xg_firewall					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	18-06-2020	7.5	A heap-based buffer overflow in the awarrensmtp component of Sophos XG Firewall v17.5 MR11 and older potentially allows an attacker to run arbitrary code remotely. **CVE ID : CVE-2020-11503**	https://community.sophos.com/b/security-blog/posts/advisory-potential-rce-through-heap-overflow-in-awarrensmtp-cve-2020-11503	H-SOP-XG_F-070820/2807
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	29-06-2020	7.5	Sophos XG Firewall 17.x through v17.5 MR12 allows a Buffer Overflow and remote code execution via the HTTP/S Bookmarks feature for clientless access. Hotfix HF062020.1 was published for all firewalls running v17.x. **CVE ID : CVE-2020-15069**	https://community.sophos.com/b/security-blog/posts/advisory-buffer-overflow-vulnerability-in-user-portal	H-SOP-XG_F-070820/2808
Supermicro					
x10drh-it					
Cross-Site Request Forgery (CSRF)	24-06-2020	9.3	The web interface on Supermicro X10DRH-iT motherboards with BIOS 2.0a and IPMI firmware 03.40 allows remote attackers to exploit a cgi/config_user.cgi CSRF issue to add new admin users. The fixed versions are BIOS 3.2 and firmware 03.88.	N/A	H-SUP-X10D-070820/2809

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15046		
tinxy					
smart_wifi_door_lock					
Authentication Bypass by Capture-replay	23-06-2020	4.3	Tinxy Door Lock with firmware before 3.2 allow attackers to unlock a door by replaying an Unlock request that occurred when the attacker was previously authorized. In other words, door-access revocation is mishandled. **CVE ID : CVE-2020-9438**	N/A	H-TIN-SMAR-070820/2810
Tp-link					
nc450					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	H-TP--NC45-070820/2811
nc260					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1	N/A	H-TP--NC26-070820/2812

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**		
nc250					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	H-TP--NC25-070820/2813
nc230					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow	N/A	H-TP--NC23-070820/2814

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13224		
nc220					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	H-TP--NC22-070820/2815
nc210					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**	N/A	H-TP--NC21-070820/2816
nc200					
Buffer Copy without Checking Size of Input ('Classic	17-06-2020	9	TP-LINK NC200 devices through 2.1.10 build 200401, NC210 devices through 1.0.10 build 200401, NC220 devices	N/A	H-TP--NC20-070820/2817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			through 1.3.1 build 200401, NC230 devices through 1.3.1 build 200401, NC250 devices through 1.3.1 build 200401, NC260 devices through 1.5.3 build_200401, and NC450 devices through 1.5.4 build 200401 have a Buffer Overflow **CVE ID : CVE-2020-13224**		
tl-wr740n					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-06-2020	3.5	On TP-Link TL-WR740N v4 and TL-WR740ND v4 devices, an attacker with access to the admin panel can inject HTML code and change the HTML context of the target pages and stations in the access-control settings via targets_lists_name or hosts_lists_name. The vulnerability can also be exploited through a CSRF, requiring no authentication as an administrator. **CVE ID : CVE-2020-14965**	N/A	H-TP--TL-W-070820/2818
tl-wr740nd					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-06-2020	3.5	On TP-Link TL-WR740N v4 and TL-WR740ND v4 devices, an attacker with access to the admin panel can inject HTML code and change the HTML context of the target pages and stations in the access-control settings via targets_lists_name or hosts_lists_name. The vulnerability can also be exploited through a CSRF,	N/A	H-TP--TL-W-070820/2819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requiring no authentication as an administrator. **CVE ID : CVE-2020-14965**		
uvd-robots					
uvd_robots					
Use of Hard-coded Credentials	24-06-2020	5	One of the wireless interfaces within MiR100, MiR200 and possibly (according to the vendor) other MiR fleet vehicles comes pre-configured in WiFi Master (Access Point) mode. Credentials to such wireless Access Point default to well known and widely spread SSID (MiR_RXXXX) and passwords (omitted). This information is also available in past User Guides and manuals which the vendor distributed. We have confirmed this flaw in MiR100 and MiR200 but it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10269**	https://github.com/aliasrobotics/RVD/issues/2566	H-UVD-UVD_-070820/2820
Use of Hard-coded Credentials	24-06-2020	5	Out of the wired and wireless interfaces within MiR100, MiR200 and other vehicles from the MiR fleet, it's possible to access the Control Dashboard on a hardcoded IP address. Credentials to such wireless interface default to well known and widely spread users (omitted) and passwords (omitted). This information is also available	https://github.com/aliasrobotics/RVD/issues/2557	H-UVD-UVD_-070820/2821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in past User Guides and manuals which the vendor distributed. This flaw allows cyber attackers to take control of the robot remotely and make use of the default user interfaces MiR has created, lowering the complexity of attacks and making them available to entry-level attackers. More elaborated attacks can also be established by clearing authentication and sending network requests directly. We have confirmed this flaw in MiR100 and MiR200 but according to the vendor, it might also apply to MiR250, MiR500 and MiR1000. **CVE ID : CVE-2020-10270**		
Exposure of Resource to Wrong Sphere	24-06-2020	5	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph to all network interfaces, wireless and wired. This is the result of a bad set up and can be mitigated by appropriately configuring ROS and/or applying custom patches as appropriate. Currently, the ROS computational graph can be accessed fully from the wired exposed ports. In combination with other flaws such as CVE-2020-10269, the computation graph can also be fetched	https://github.com/aliasrobotics/RVD/issues/2555	H-UVD-UVD_-070820/2822

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and interacted from wireless networks. This allows a malicious operator to take control of the ROS logic and correspondingly, the complete robot given that MiR's operations are centered around the framework (ROS). **CVE ID : CVE-2020-10271**		
Missing Authentication for Critical Function	24-06-2020	10	MiR100, MiR200 and other MiR robots use the Robot Operating System (ROS) default packages exposing the computational graph without any sort of authentication. This allows attackers with access to the internal wireless and wired networks to take control of the robot seamlessly. In combination with CVE-2020-10269 and CVE-2020-10271, this flaw allows malicious actors to command the robot at desire. **CVE ID : CVE-2020-10272**	https://github.com/aliasrobotics/RVD/issues/2554	H-UVD-UVD_-070820/2823
Missing Encryption of Sensitive Data	24-06-2020	5	MiR controllers across firmware versions 2.8.1.1 and before do not encrypt or protect in any way the intellectual property artifacts installed in the robots. This flaw allows attackers with access to the robot or the robot network (while in combination with other flaws) to retrieve and easily exfiltrate all installed intellectual property and	https://github.com/aliasrobotics/RVD/issues/2560	H-UVD-UVD_-070820/2824

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data. **CVE ID : CVE-2020-10273**		
Improper Authentication	24-06-2020	5	The BIOS onboard MiR's Computer is not protected by password, therefore, it allows a Bad Operator to modify settings such as boot order. This can be leveraged by a Malicious operator to boot from a Live Image. **CVE ID : CVE-2020-10278**	https://github.com/aliasrobotics/RVD/issues/2561	H-UVD-UVD_-070820/2825
Incorrect Default Permissions	24-06-2020	7.5	MiR robot controllers (central computation unit) makes use of Ubuntu 16.04.2 an operating system, Thought for desktop uses, this operating system presents insecure defaults for robots. These insecurities include a way for users to escalate their access beyond what they were granted via file creation, access race conditions, insecure home directory configurations and defaults that facilitate Denial of Service (DoS) attacks. **CVE ID : CVE-2020-10279**	https://github.com/aliasrobotics/RVD/issues/2569	H-UVD-UVD_-070820/2826
uvd					
Information Exposure	24-06-2020	5.5	The access tokens for the REST API are directly derived (sha256 and base64 encoding) from the publicly available default credentials from the Control Dashboard (refer to CVE-2020-10270 for related flaws). This flaw in combination with CVE-2020-10273 allows any	https://github.com/aliasrobotics/RVD/issues/2556	H-UVD-UVD-070820/2827

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker connected to the robot networks (wired or wireless) to exfiltrate all stored data (e.g. indoor mapping images) and associated metadata from the robot's database. **CVE ID : CVE-2020-10274**		
Inadequate Encryption Strength	24-06-2020	7.5	The access tokens for the REST API are directly derived from the publicly available default credentials for the web interface. Given a USERNAME and a PASSWORD, the token string is generated directly with base64(USERNAME:sha256(PASSWORD)). An unauthorized attacker inside the network can use the default credentials to compute the token and interact with the REST API to exfiltrate, infiltrate or delete data. **CVE ID : CVE-2020-10275**	https://github.com/aliasrobotics/RVD/issues/2565	H-UVD-UVD-070820/2828
Use of Hard-coded Credentials	24-06-2020	7.5	The password for the safety PLC is the default and thus easy to find (in manuals, etc.). This allows a manipulated program to be uploaded to the safety PLC, effectively disabling the emergency stop in case an object is too close to the robot. Navigation and any other components dependent on the laser scanner are not affected (thus it is hard to detect	https://github.com/aliasrobotics/RVD/issues/2558	H-UVD-UVD-070820/2829

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before something happens) though the laser scanner configuration can also be affected altering further the safety of the device. **CVE ID : CVE-2020-10276**		
Information Exposure	24-06-2020	4.6	There is no mechanism in place to prevent a bad operator to boot from a live OS image, this can lead to extraction of sensible files (such as the shadow file) or privilege escalation by manually adding a new user with sudo privileges on the machine. **CVE ID : CVE-2020-10277**	https://github.com/aliasrobotics/RVD/issues/2562	H-UVD-UVD-070820/2830
Improper Resource Shutdown or Release	24-06-2020	5	The Apache server on port 80 that host the web interface is vulnerable to a DoS by spamming incomplete HTTP headers, effectively blocking the access to the dashboard. **CVE ID : CVE-2020-10280**	https://github.com/aliasrobotics/RVD/issues/2568	H-UVD-UVD-070820/2831
ZTE					
netnumen_u31_r10					
N/A	24-06-2020	5.2	The version V12.17.20T115 of ZTE U31R20 product is impacted by a design error vulnerability. An attacker could exploit the vulnerability to log in to the FTP server to tamper with the password, and illegally download, modify, upload, or delete files, causing improper operation of the network management	http://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1013043	H-ZTE-NETN-070820/2832

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system and equipment. This affects: NetNumenU31R20 V12.17.20T115 **CVE ID : CVE-2020-6870**		
Zyxel					
wap6806					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-06-2020	5	Zyxel Armor X1 WAP6806 1.00(ABAL.6)C0 devices allow Directory Traversal via the images/eaZy/ URI. **CVE ID : CVE-2020-14461**	N/A	H-ZYX-WAP6-070820/2833