National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures(CVE) Report 16 - 30 Sep 2019 Vol. 06 No. 18									
Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Application						
5none									
nonecms									
Cross-Site Request Forgery (CSRF)	23-09-2019	5.8	NoneCMS v1.3 has CSRF in public/index.php/admin/ad min/dele.html, as demonstrated by deleting the admin user. CVE ID : CVE-2019-16721	N/A	A-5NO-NONE- 141019/1				
Advantech									
Webaccess/h	mi_designer								
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-09-2019	5	In Advantech WebAccess/HMI Designer 2.1.9.31, Data from a Faulting Address controls Code Flow starting at PM_V3!CTagInfoThreadBase: :GetNICInfo+0x000000000 512918. CVE ID : CVE-2019-16899	N/A	A-ADV- WEBA- 141019/2				
Improper Restriction of Operations within the Bounds of a Memory Buffer	25-09-2019	5	Advantech WebAccess/HMI Designer 2.1.9.31 has a User Mode Write AV starting at MSVCR90!memcpy+0x0000 00000000015c. CVE ID : CVE-2019-16900	N/A	A-ADV- WEBA- 141019/3				
Improper Handling of Exceptional Conditions	25-09-2019	5	Advantech WebAccess/HMI Designer 2.1.9.31 has Exception Handler Chain corruption starting at Unknown Symbol @	N/A	A-ADV- WEBA- 141019/4				

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0x00000000000000000 called from ntdll!RtlRaiseStatus+0x0000 000000000b4.		
			CVE ID : CVE-2019-16901		
webaccess			L		
Incorrect Authorizatio n	18-09-2019	9	In WebAccess, versions 8.4.1 and prior, an improper authorization vulnerability may allow an attacker to disclose sensitive information, cause improper control of generation of code, which may allow remote code execution or cause a system crash.	N/A	A-ADV- WEBA- 141019/5
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	18-09-2019	6.5	CVE ID : CVE-2019-13550 In WebAccess versions 8.4.1 and prior, multiple command injection vulnerabilities are caused by a lack of proper validation of user-supplied data and may allow arbitrary file deletion and remote code execution. CVE ID : CVE-2019-13552	N/A	A-ADV- WEBA- 141019/6
Improper Restriction of Operations within the Bounds of a Memory Buffer	18-09-2019	6.5	In WebAccess versions 8.4.1 and prior, multiple stack- based buffer overflow vulnerabilities are caused by a lack of proper validation of the length of user-supplied data. Exploitation of these vulnerabilities may allow remote code execution. CVE ID : CVE-2019-13556	N/A	A-ADV- WEBA- 141019/7
Improper Control of	18-09-2019	9	In WebAccess versions 8.4.1 and prior, an exploit	N/A	A-ADV- WEBA-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				r						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIPC	D
Generation of Code ('Code Injection')			executed over the network may cause improper control of generation of code, which may allow remote code execution, data exfiltration, or cause a system crash.			141019/	8
			CVE ID : CVE-2019-13558				
Apache							
tapestry			Manipulating classpath asset				
Deserializati on of Untrusted Data	16-09-2019	7.5	file URLs, an attacker could guess the path to a known file in the classpath and have it downloaded. If the attacker found the file with the value of the tapestry.hmac-passphrase configuration symbol, most probably the webapp's AppModule class, the value of this symbol could be used to craft a Java deserialization attack, thus running malicious injected Java code. The vector would be the t:formdata parameter from the Form component. CVE ID : CVE-2019-0195	N/A		A-APA-TA 141019/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-09-2019	5	Tapestry processes assets `/assets/ctx` using classes chain `StaticFilesFilter -> AssetDispatcher -> ContextResource`, which doesn't filter the character `\`, so attacker can perform a path traversal attack to read any files on Windows platform. CVE ID : CVE-2019-0207	N/A		A-APA-TA 141019/	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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	16-09-2019	6.8	The code which checks HMAC in form submissions used String.equals() for comparisons, which results in a timing side channel for the comparison of the HMAC signatures. This could lead to remote code execution if an attacker is able to determine the correct signature for their payload. The comparison should be done with a constant time algorithm instead. CVE ID : CVE-2019-10071		A-APA-TAPE- 141019/11
subversion	I				
Improper Input Validation	26-09-2019	5	In Apache Subversion versions up to and including 1.9.10, 1.10.4, 1.12.0, Subversion's svnserve server process may exit when a client sends certain sequences of protocol commands. This can lead to disruption for users of the server. CVE ID : CVE-2019-0203	N/A	A-APA-SUBV- 141019/12
http_server					
Use After Free	26-09-2019	6.4	In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown. CVE ID : CVE-2019-10082	N/A	A-APA-HTTP- 141019/13
Improper Neutralizatio n of Input	26-09-2019	4.3	In Apache HTTP Server 2.4.0-2.4.39, a limited cross- site scripting issue was	N/A	A-APA-HTTP- 141019/14
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9</mark> -10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed. CVE ID : CVE-2019-10092		
NULL Pointer Dereference	26-09-2019	6	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients. CVE ID : CVE-2019-10097	N/A	A-APA-HTTP- 141019/15
URL Redirection to Untrusted Site ('Open Redirect')	25-09-2019	5.8	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self- referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL. CVE ID : CVE-2019-10098	N/A	A-APA-HTTP- 141019/16

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jspwiki	I				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the Page Revision History, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-10087	N/A	A-APA-JSPW- 141019/17
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the WYSIWYG editor, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-10089	N/A	A-APA-JSPW- 141019/18
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the plain editor, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim.	N/A	A-APA-JSPW- 141019/19

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

Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')23-09-20194.3On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-12404N/AA-APA-JSPW- 141019/20Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')23-09-20194.3On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the remember parameter on some of the JSPs, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-12407N/AA-APA-JSPW- 141019/21Improper Neutralizatio n of Input Page Generation ('Cross-site Scripting')23-09-20194.3On Apache JSPWiki, up to version 2.110.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the remember parameter on some of the JSPs, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-12407N/AApereo Lessed Candend StringUtia Candend StringUtia Random Random Random Random23-09-2019S.5Multiple classes used within Apereo CAS before release 6.1.0-RCS makes use of apache commons-lang3 RandomStringUtias for token<	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')23-09-20194.3version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to InfoContent.jsp, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim.N/AA-APA-JSPW- 141019/20Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')23-09-20194.3On Apache JSPWiki, up to version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the remember parameter on some of the JSPs, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-12407N/AA-APA-JSPW- 141019/21Apereo Central_authentication_service4.3Sme of the JSPs, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-12407N/AA-APA-JSPW- 141019/21Use of capity weak Pseudo- Random Number (enerator (PRNG)23-09-20195.5Multiple classes used within Apereo CAS before release 6.10-RCS makes use of apache commons-lang3 Random StringUtils for token and ID generation which makes them predictable due to RandomStringUtils PRNG's algorithm not beingN/AA-APE-CENT- 141019/22				CVE ID : CVE-2019-10090		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')23-09-20194.3version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the remember parameter on some of the JSPs, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. CVE ID : CVE-2019-12407N/AA-APA-JSPW- 141019/21ApereoCentral_authentication_serviceUse of Cryptographi cally Weak Pseudo- Random Number (PRNG)23-09-20195.5Multiple classes used within Apereo CAS before release 6.1.0-RCS makes use of apache commons-lang3 RandomStringUtils for token and ID generation which makes them predictable due to RandomStringUtils PRNG's algorithm not beingN/AA-APE-CENT- 141019/22	Neutralizatio n of Input During Web Page Generation ('Cross-site	23-09-2019	4.3	version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to InfoContent.jsp, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim.	N/A	-
central_authentication_service Use of Cryptographi cally Weak Pseudo- Random Number Generator (PRNG) A-APE-CENT- 5.5 Multiple classes used within Apereo CAS before release 6.1.0-RC5 makes use of apache commons-lang3 RandomStringUtils for token and ID generation which makes them predictable due to RandomStringUtils PRNG's algorithm not being N/A A-APE-CENT- 141019/22	Neutralizatio n of Input During Web Page Generation ('Cross-site	23-09-2019	4.3	version 2.11.0.M4, a carefully crafted plugin link invocation could trigger an XSS vulnerability on Apache JSPWiki, related to the remember parameter on some of the JSPs, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim.	N/A	-
Use of Cryptographi cally Weak Pseudo- Random Number Generator (PRNG)23-09-2019S.5Multiple classes used within Apereo CAS before release 6.1.0-RC5 makes use of apache commons-lang3 RandomStringUtils for token and ID generation which makes them predictable due to RandomStringUtils PRNG's algorithm not beingN/AA-APE-CENT- 141019/22	Apereo					
Ose of Cryptographi cally Weak Pseudo- Random Number Generator (PRNG)Apereo CAS before release 6.1.0-RC5 makes use of apache commons-lang3 RandomStringUtils for token and ID generation which makes them predictable due to RandomStringUtils PRNG's algorithm not beingN/AA-APE-CENT- 141019/22CV Scoring Scale0.11.22.33.44.55.66.77.88.99.10	central_authe	entication_ser	vice			
	Cryptographi cally Weak Pseudo- Random Number Generator	23-09-2019	5.5	Apereo CAS before release 6.1.0-RC5 makes use of apache commons-lang3 RandomStringUtils for token and ID generation which makes them predictable due to RandomStringUtils	N/A	
	CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-6	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cryptographically strong.		
			CVE ID : CVE-2019-10754		
aspose					
aspose.pdf_fo	r_c++				
Use After Free	18-09-2019	7.5	An uninitialized memory access vulnerability exists in the way Aspose.PDF 19.2 for C++ handles invalid parent object pointers. A specially crafted PDF can cause a read and write from uninitialized memory, resulting in memory corruption and possibly arbitrary code execution. To trigger this vulnerability, a specifically crafted PDF document needs to be processed by the targe application. CVE ID : CVE-2019-5067	https://ww w.talosintell igence.com/ vulnerabilit y_reports/T ALOS-2019- 0856	A-ASP-ASPO- 141019/23
Use After Free	18-09-2019	6.5	An exploitable Use-After- Free vulnerability exists in the way FunctionType 0 PDF elements are processed in Aspose.PDF 19.2 for C++. A specially crafted PDF can cause a dangling heap pointer, resulting in a use- after-free. An attacker can send a malicious PDF to trigger this vulnerability. CVE ID : CVE-2019-5042	https://ww w.talosintell igence.com/ vulnerabilit y_reports/T ALOS-2019- 0809	A-ASP-ASPO- 141019/24
Use After Free	18-09-2019	7.5	An exploitable use-after-free vulnerability exists in the way LZW-compressed streams are processed in Aspose.PDF 19.2 for C++. A specially crafted PDF can cause a dangling heap	<pre>https://ww w.talosintell igence.com/ vulnerabilit y_reports/T ALOS-2019-</pre>	A-ASP-ASPO- 141019/25
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer, resulting in a use- after-free condition. To trigger this vulnerability, a specifically crafted PDF document needs to be processed by the target application. CVE ID : CVE-2019-5066	0855	
Atlassian					
jira					
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	19-09-2019	9	The Jira Importers Plugin in Atlassian Jira Server and Data Cente from version with 7.0.10 before 7.6.16, from 7.7.0 before 7.13.8, from 8.1.0 before 8.1.3, from 8.2.0 before 8.2.5, from 8.3.0 before 8.3.4 and from 8.4.0 before 8.4.1 allows remote attackers with Administrator permissions to gain remote code execution via a template injection vulnerability through the use of a crafted PUT request. CVE ID : CVE-2019-15001	N/A	A-ATL-JIRA- 141019/26
bitbucket					
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	19-09-2019	6.8	The commit diff rest endpoint in Bitbucket Server and Data Center before 5.16.10 (the fixed version for 5.16.x), from 6.0.0 before 6.0.10 (the fixed version for 6.0.x), from 6.1.0 before 6.1.8 (the fixed version for 6.1.x), from 6.2.0 before 6.2.6 (the fixed version for 6.2.x), from 6.3.0 before 6.3.5 (the fixed version for		A-ATL-BITB- 141019/27
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.3.x), from 6.4.0 before 6.4.3 (the fixed version for 6.4.x), and from 6.5.0 before 6.5.2 (the fixed version for 6.5.x) allows remote attackers who have permission to access a repository, if public access is enabled for a project or repository then attackers are able to exploit this issue anonymously, to read the contents of arbitrary files on the system and execute commands via injecting additional arguments into git commands. CVE ID : CVE-2019-15000		
jira_service_d	esk_server				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-09-2019	4.3	The Customer Context Filter in Atlassian Jira Service Desk Server and Jira Service Desk Data Center before version 3.9.16, from version 3.10.0 before version 3.16.8, from version 4.0.0 before version 4.1.3, from version 4.2.0 before version 4.2.5, from version 4.3.0 before version 4.3.4, and version 4.4.0 allows remote attackers with portal access to view arbitrary issues in Jira Service Desk projects via a path traversal vulnerability. Note that when the 'Anyone can email the service desk or raise a request in the portal' setting is enabled, an attacker can grant	N/A	A-ATL-JIRA- 141019/28
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			themselves portal access, allowing them to exploit the vulnerability.		
			CVE ID : CVE-2019-14994		
axiosys					
bento4					
NULL Pointer Dereference	16-09-2019	4.3	Bento4 1.5.1-628 has a NULL pointer dereference in AP4_ByteStream::ReadUI32 in Core/Ap4ByteStream.cpp when called from the AP4_TrunAtom class. CVE ID : CVE-2019-16349	N/A	A-AXI-BENT- 141019/29
beego	I				I
beego					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	1.9	The File Session Manager in Beego 1.10.0 allows local users to read session files because there is a race condition involving file creation within a directory with weak permissions. CVE ID : CVE-2019-16354	N/A	A-BEE-BEEG- 141019/30
Incorrect Default Permissions	16-09-2019	2.1	The File Session Manager in Beego 1.10.0 allows local users to read session files because of weak permissions for individual files. CVE ID : CVE-2019-16355	N/A	A-BEE-BEEG- 141019/31
Bluestacks					
bluestacks					
Information Exposure	24-09-2019	4.9	An issue was discovered in BlueStacks 4.110 and below on macOS and on 4.120 and below on Windows. BlueStacks employs Android	https://sup port.bluesta cks.com/hc /en- us/articles/	A-BLU-BLUE- 141019/32
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			running in a virtual machine (VM) to enable Android apps to run on Windows or MacOS. Bug is in a local arbitrary file read through a system service call. The impacted method runs with System admin privilege and if given the file name as parameter returns you the content of file. A malicious app using the affected method can then read the content of any system file which it is not authorized to read	360033484 132- BlueStacks- fails-to- restrict- access- permissions	
			CVE ID : CVE-2019-14220		
Cacti					
cacti					
Authorizatio n Bypass Through User- Controlled Key	23-09-2019	4	In Cacti through 1.2.6, authenticated users may bypass authorization checks (for viewing a graph) via a direct graph_json.php request with a modified local_graph_id parameter.	N/A	A-CAC-CACT- 141019/33
			CVE ID : CVE-2019-16723		
Centreon					
centreon					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	25-09-2019	7.5	SQL injection vulnerabilities in Centreon through 19.04 allow attacks via the svc_id parameter in include/monitoring/status/ Services/xml/makeXMLFor OneService.php. CVE ID : CVE-2019-16194	N/A	A-CEN-CENT- 141019/34
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				12						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
checklist	I	<u> </u>			•
checklist					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	19-09-2019	4.3	An XSS issue was discovered in the checklist plugin before 1.1.9 for WordPress. The fill parameter is not correctly filtered in the checklist- icon.php file, and it is possible to inject JavaScript code. CVE ID : CVE-2019-16525	N/A	A-CHE-CHEC- 141019/35
cloudfoundry	,				
cf-deploymen	it				
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	23-09-2019	5.5	Cloud Foundry NFS Volume Service, 1.7.x versions prior to 1.7.11 and 2.x versions prior to 2.3.0, is vulnerable to LDAP injection. A remote authenticated malicious space developer can potentially inject LDAP filters via service instance creation, facilitating the malicious space developer to deny service or perform a dictionary attack. CVE ID : CVE-2019-11277	https://ww w.cloudfou ndry.org/bl og/cve- 2019- 11277	A-CLO-CF-D- 141019/36
code42	I			L	
code42					
Unrestricted Upload of File with Dangerous Type	17-09-2019	7.5	In Code42 Enterprise 6.7.5 and earlier, 6.8.4 through 6.8.8, and 7.0.0 a vulnerability has been identified that may allow arbitrary files to be uploaded to Code42 servers and executed. This vulnerability could allow an attacker to	N/A	A-COD-CODE- 141019/37
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Descri	iption & CVE	ID	Pat	tch	NCIIP	CID
			create directories and save files on Code42 servers, which could potentially lead to code execution.						
			CVE ID : C	VE-2019-1	5131				
Codesys									
control_for_b	eaglebone								
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. CVE ID : CVE-2019-9008		N/A		A-COD- 141019		
control_for_e	mpc-a/imx6							L	
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. CVE ID : CVE-2019-9008			N/A		A-COD- 141019	
control_for_io	ot2000								
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	3S-Smart (through 3. with low p	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime.		N/A		A-COD- 141019	
control_for_p	fc100								
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. CVE ID : CVE-2019-9008			N/A		A-COD- 141019	
control_for_p	fc200								
Incorrect	17-09-2019	6.5	An issue w	as discover	red in	N/A		A-COD-	CONT-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	h	NCIIPC ID
Permission Assignment for Critical Resource			3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime.			141019/42
			CVE ID : CVE-2019-9008			
control_for_ra	aspberry_pi					I
Incorrect Permission Assignment for Critical Resource	17-09-2019	6.5	An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime. CVE ID : CVE-2019-9008	N/A		A-COD-CONT 141019/43
codesys						
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	17-09-2019	6.8	3S-Smart Software Solutions GmbH CODESYS V3 Library Manager, all versions prior to 3.5.15.0, allows the system to display active library content without checking its validity, which may allow the contents of manipulated libraries to be displayed or executed. The issue also exists for source libraries, but 3S-Smart Software Solutions GmbH strongly recommends distributing compiled libraries only. CVE ID : CVE-2019-13538	N/A		A-COD-CODE 141019/44
cure53				1		
dompurify						
Improper Neutralizatio n of Input During Web Page Generation	24-09-2019	4.3	DOMPurify before 2.0.1 allows XSS because of innerHTML mutation XSS (mXSS) for an SVG element or a MATH element, as demonstrated by Chrome	N/A		A-CUR-DOMP 141019/45
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 <mark>9</mark> -10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
('Cross-site			and S	afari.						
Scripting')			CVE I	D : CVE-	2019-1	6728				
devise_token	_auth_project									
devise_token	_auth									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	24-09-2019	4.3	Devis 1.1.2. endpo Reflec Script messa Unaut can cr a mali paylo brows fallba the or contro	sue was o e Token The omi- bint is vu cted Cros- cing (XSS age para- caft a UR icious Ja- ad in the ser. This ck_rendo nniauth oller. D : CVE-	Auth thi niauth fa Inerable ss Site () throug meter. ted attac that en vaScript e victim' affects the callback	rough ailure e to gh the ckers xecutes c s the od in ts	N/A		A-DEV-I 141019	
digimute	<u>I</u>									
ogma_cms										
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	3.5	creati	Ogma CMS 0.5 has XSS via creation of a new blog. CVE ID : CVE-2019-16661		N/A		A-DIG-C 141019		
dnnsoftware										
dotnetnuke										
Improper Neutralizatio n of Input During Web Page Generation	26-09-2019	4.3	Stored Cross-Site Scripting in DotNetNuke (DNN) Version before 9.4.0 allows remote attackers to store and embed the malicious script into the admin				N/A		A-DNN- DOTN- 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
('Cross-site Scripting')			notification page. The exploit could be used to perfom any action with admin privileges such as managing content, adding users, uploading backdoors to the server, etc. Successful exploitation occurs when an admin user visits a notification page with stored cross-site scripting. CVE ID : CVE-2019-12562						
Docker				2017 1					
docker									
Incorrect Authorizatio n	25-09-2019	5	runc through used in Docke 19.03.2-ce and products, allo restriction by libcontainer/n incorrectly ch targets, and th Docker image over a /proc co	er throug d other ws AppA pass bec rootfs_lin ecks mo nus a ma can mou directory	h armor ause nux.go unt licious int	N/A		A-DOC-1 141019	
Dolibarr						<u> </u>			
dolibarr									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting') Improper	16-09-2019	4.3	In htdocs/societe/card.php in Dolibarr 10.0.1, the value of the User-Agent HTTP header is copied into the HTML document as plain text between tags, leading to XSS. CVE ID : CVE-2019-16197 Dolibarr 9.0.5 has stored XSS			N/A		A-DOL-1 141019 A-DOL-1	/50
Neutralizatio n of Input	27-09-2019	3.5	in a User Note section to note.php. A user with no			N/A		A-DOL- 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			privileges can inject script to attack the admin. CVE ID : CVE-2019-16686		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-09-2019	3.5	Dolibarr 9.0.5 has stored XSS in a User Profile in a Signature section to card.php. A user with the "Create/modify other users, groups and permissions" privilege can inject script and can also achieve privilege escalation. CVE ID : CVE-2019-16687	N/A	A-DOL-DOLI- 141019/52
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	27-09-2019	3.5	Dolibarr 9.0.5 has stored XSS in an Email Template section to mails_templates.php. A user with no privileges can inject script to attack the admin. (This stored XSS can affect all types of user privilege from Admin to users with no permissions.) CVE ID : CVE-2019-16688	N/A	A-DOL-DOLI- 141019/53
e2fsprogs_pro	oject				
e2fsprogs					
Out-of- bounds Write	24-09-2019	4.6	An exploitable code execution vulnerability exists in the quota file functionality of E2fsprogs 1.45.3. A specially crafted ext4 partition can cause an out-of-bounds write on the heap, resulting in code execution. An attacker can corrupt a partition to trigger this vulnerability.	N/A	A-E2F-E2FS- 141019/54

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5094		
Eclipse	I			I	I
mosquitto					
Use After Free	18-09-2019	5.5	If an MQTT v5 client connects to Eclipse Mosquitto versions 1.6.0 to 1.6.4 inclusive, sets a last will and testament, sets a will delay interval, sets a session expiry interval, and the will delay interval is set longer than the session expiry interval, then a use after free error occurs, which has the potential to cause a crash in some situations. CVE ID : CVE-2019-11778	https://bug s.eclipse.org /bugs/sho w_bug.cgi?i d=551162	A-ECL-MOSQ- 141019/55
Improper Check for Unusual or Exceptional Conditions	19-09-2019	4	In Eclipse Mosquitto 1.5.0 to 1.6.5 inclusive, if a malicious MQTT client sends a SUBSCRIBE packet containing a topic that consists of approximately 65400 or more '/' characters, i.e. the topic hierarchy separator, then a stack overflow will occur. CVE ID : CVE-2019-11779	N/A	A-ECL-MOSQ- 141019/56
egpp					
sistema_integ	rado_de_gest	ion_aca	idemica		
Improper Neutralizatio n of Special Elements used in an SQL Command	16-09-2019	7.5	In Escuela de Gestion Publica Plurinacional (EGPP) Sistema Integrado de Gestion Academica (GESAC) v1, the username parameter of the authentication form is vulnerable to SQL injection,	N/A	A-EGP-SIST- 141019/57
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL			allowing attackers to access the database.		
Injection')			CVE ID : CVE-2019-16264		
Embedthis			CVE ID : CVE-2019-10204		
-					
goahead					T
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	20-09-2019	5	An issue was discovered in Embedthis GoAhead 2.5.0. Certain pages (such as goform/login and config/log_off_page.htm) create links containing a hostname obtained from an arbitrary HTTP Host header sent by an attacker. This could potentially be used in a phishing attack. CVE ID : CVE-2019-16645	N/A	A-EMB- GOAH- 141019/58
emlog					
emlog					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-09-2019	7.5	emlog through 6.0.0beta has an arbitrary file deletion vulnerability via an admin/data.php?action=dell _all_bak request with directory traversal sequences in the bak[] parameter. CVE ID : CVE-2019-16868	N/A	A-EML-EMLO- 141019/59
F5					
big-ip_access	_policy_mana	ger			
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1,	N/A	A-F5-BIG 141019/60
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIPC ID
			the Configuration utility login page may not follow best security practices when handling a malicious request.			
			CVE ID : CVE-2019-6651			
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654	N/A		A-F5-BIG 141019/61
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1- 11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. CVE ID : CVE-2019-6655	N/A		A-F5-BIG 141019/62
big-ip_advanc	ed_firewall_n	nanage	r	- -		
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when	N/A		A-F5-BIG 141019/63
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling a malicious request.		
			CVE ID : CVE-2019-6651		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654	N/A	A-F5-BIG 141019/64
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1- 11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. CVE ID : CVE-2019-6655	N/A	A-F5-BIG 141019/65
big-ip_analyti	CS				
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request.	N/A	A-F5-BIG 141019/66

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				22						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6651		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654	N/A	A-F5-BIG 141019/67
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1- 11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. CVE ID : CVE-2019-6655	N/A	A-F5-BIG 141019/68
big-ip_applica	ation_accelera	tion_n	lanager		
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651	N/A	A-F5-BIG 141019/69
Improper Input	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5,	N/A	A-F5-BIG
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654		141019/70
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1- 11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. CVE ID : CVE-2019-6655	N/A	A-F5-BIG 141019/71
big-ip_applica	ation_security	_mana	ger		
Information Exposure	20-09-2019	5.8	F5 BIG-IP ASM 15.0.0, 14.1.0-14.1.0.6, 14.0.0- 14.0.0.5, 13.0.0-13.1.1.5, 12.1.0-12.1.4.1, 11.6.0- 11.6.4, and 11.5.1-11.5.9 may expose sensitive information and allow the system configuration to be modified when using non- default settings. CVE ID : CVE-2019-6650	https://sup port.f5.com /csp/article /K0428004 2	A-F5-BIG 141019/72
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1,	N/A	A-F5-BIG 141019/73
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 Configuration utility login page may not follow best security practices when handling a malicious request.		
			CVE ID : CVE-2019-6651		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654	N/A	A-F5-BIG 141019/74
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1- 11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. CVE ID : CVE-2019-6655	N/A	A-F5-BIG 141019/75
big-ip_domain	n_name_syste	m			
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when	N/A	A-F5-BIG 141019/76
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			handl reque	ing a ma	alicious					
			-	D : CVE-	2019-6	651				
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654				N/A		A-F5-BI 141019	
big-ip_edge_g	ateway									
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651		N/A		A-F5-BI 141019			
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management				N/A		A-F5-BI 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
			attack syster proce	ace). Th kers on a m to force ssing pa ed source	in adjac ce BIG-I ickets w	ent P into ith				
			CVE I	D : CVE-	2019-6	654				
big-ip_fraud_p	protection_se	rvice					1			
Information Exposure Through Discrepancy	25-09-2019	5	14.1.0 13.0.0 12.1.4 IQ 7.0 5.4.0, Enter the Co login best s	G-IP 15.0 0.6, 14.0 0-13.1.1. 0.13.1.1. 0.0, 6.0.0 iWorkfl prise Ma page ma page ma security j ing a ma	.0-14.0.0 5, 12.1.0 .1-11.6.4 -6.1.0,5 ow 2.3.0 anager 3 tion util anager 5 tion util anager 5	0.5,)- 4, BIG- .2.0-), and 3.1.1, lity llow	N/A		A-F5-BI 141019	
			CVE I	D : CVE·	2019-6	651				
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654				N/A		A-F5-BI 141019	
big-ip_global_	traffic_manag	ger	1				1			
Information Exposure Through	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG-				N/A		A-F5-BI 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Discrepancy			IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651		
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654	N/A	A-F5-BIG 141019/83
big-ip_link_co	ontroller				
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651	N/A	A-F5-BIG 141019/84
Improper Input	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5,	N/A	A-F5-BIG 141019/85
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	³ 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIF	'C ID
Validation			and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654				
big-ip_local_tr	raffic_manage	r					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651	N/A		A-F5-BI 141019	
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses.	N/A		A-F5-BI 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				29						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6654		
big-ip_policy_	enforcement_	manag	ger	<u> </u>	
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651	N/A	A-F5-BIG 141019/88
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654	N/A	A-F5-BIG 141019/89
Information Exposure	25-09-2019	4.3	On versions 13.0.0-13.1.0.1, 12.1.0-12.1.4.1, 11.6.1- 11.6.4, and 11.5.1-11.5.9, BIG-IP platforms where AVR, ASM, APM, PEM, AFM, and/or AAM is provisioned may leak sensitive data. CVE ID : CVE-2019-6655	N/A	A-F5-BIG 141019/90
big-ip_webac	celerator			I	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				20						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651	N/A	A-F5-BIG 141019/91
Improper Input Validation	25-09-2019	3.3	On versions 14.0.0-14.1.2, 13.0.0-13.1.3, 12.1.0-12.1.5, and 11.5.1-11.6.5, the BIG-IP system fails to perform Martian Address Filtering (As defined in RFC 1812 section 5.3.7) on the control plane (management interface). This may allow attackers on an adjacent system to force BIG-IP into processing packets with spoofed source addresses. CVE ID : CVE-2019-6654	N/A	A-F5-BIG 141019/92
enterprise_m	anager				
Information Exposure Through Discrepancy	spoofed source addresses. CVE ID : CVE-2019-6654 In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow		14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility	N/A	A-F5-ENTE- 141019/93

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				21						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request.		
			CVE ID : CVE-2019-6651		
big-iq_central	lized_manage	ment			
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0- 5.4.0, iWorkflow 2.3.0, and Enterprise Manager 3.1.1, the Configuration utility login page may not follow best security practices when handling a malicious request. CVE ID : CVE-2019-6651	0.6, 14.0.0-14.0.0.5, 0.0-13.1.1.5, 12.1.0- 4.1, 11.5.1-11.6.4, BIG- 0.0.0, 6.0.0-6.1.0,5.2.0- 0, iWorkflow 2.3.0, and erprise Manager 3.1.1, Configuration utility n page may not follow a security practices when dling a malicious test. ID : CVE-2019-6651	
Improper Authenticati on	25-09-2019	6.4	In BIG-IQ 6.0.0-6.1.0, services for stats do not require authentication nor do they implement any form of Transport Layer Security (TLS). CVE ID : CVE-2019-6652	N/A	A-F5-BIG 141019/95
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	There is a Stored Cross Site Scripting vulnerability in the undisclosed page of a BIG-IQ 6.0.0-6.1.0 or 5.2.0-5.4.0 system. The attack can be stored by users granted the Device Manager and Administrator roles. CVE ID : CVE-2019-6653	N/A	A-F5-BIG 141019/96
iworkflow					
Information Exposure Through Discrepancy	25-09-2019	5	In BIG-IP 15.0.0, 14.1.0- 14.1.0.6, 14.0.0-14.0.0.5, 13.0.0-13.1.1.5, 12.1.0- 12.1.4.1, 11.5.1-11.6.4, BIG- IQ 7.0.0, 6.0.0-6.1.0,5.2.0-	N/A	A-F5-IWOR- 141019/97
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & C	VE ID	Pat	tch	NCIIP	C ID
			5.4.0, iWorkflow 2. Enterprise Manage the Configuration u login page may not best security praction handling a malicion request. CVE ID : CVE-2019	r 3.1.1, itility follow ices when is				
firegiant								
wix_toolset								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	19-09-2019	5.8	An issue was discor DTF in FireGiant W Toolset before 3.11 Microsoft.Deploym ression.Cab.dll and Microsoft.Deploym ression.Zip.dll allow directory traversal CAB or ZIP archive extraction, because name of an archive with a/ sequence concatenated with destination path. CVE ID : CVE-2019	YiX 2. ent.Comp ent.Comp w during e the full file (even) is the	N/A		A-FIR-W 141019	_
forcepoint								
vpn_client								
Unquoted Search Path or Element	20-09-2019	7.2	Forcepoint VPN Cli Windows versions than 6.6.1 have and search path vulner This enables local p escalation to SYSTI By default, only loc administrators can executables to the vulnerable director Forcepoint thanks Hadar of SafeBreac	https:, port.fc oint.cc BArtic =0000 5	orcep om/K cle?id	A-FOR-V 141019	_	
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5		1	7-8		

Insufficient Session Expiration17-09-20192.1A flaw was found in FreeIPA versions 4.5.0 and later. Session cookies were retained in the cache after logout. An attacker could abuse this flaw if they obtain previously valid session cookies and can use this to gain access to the session. CVE ID : CVE-2019-14826https://bug zilla.redhat. com/show_ bug.cgi?id= CVE-2019- 14826A-FRE-FREE- 141019/100geautomationIf-09-20195Emerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gilacmsImproper Limitation of a Pathname to a21-09-20194Gila CMS before 1.11.1 allows admin/fm?f=/ directory traversal, leadingN/AA-GIL-GILA-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Session ExpirationInterpret IterpretIterpret IterpretInsufficient Session Expiration17-09-2019Image: Pretion of the						
FreeipafreeipafreeipaInsufficient Session17-09-2019A flaw was found in FreeIPA versions 4.5.0 and later. Session cookies were retained in the cache after logut. An attacker could abuse this flaw if they obtain previously valid session. CVE ID : CVE-2019-14826A-FRE-FREE- 141019/100geautomationEmerson GE Automation ProficyA-FRE-FREE- tain access to the session. CVE ID : CVE-2019-14826A-FRE-FREE- tain access to the session. CVE ID : CVE-2019-14826Improper Input Validation16-09-20195Emerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101glacmsImproper Limitation of a Pathname to a Restricted Directory (Path Traversal')21-09-2019AGilla CMS before 1.11.1 allows admin/fm/?f=/ directory traversal, leading to Local File Inclusion. CVE ID : CVE-2019-16679N/AA-GIL-GILA- 141019/102						
freeipaInsufficient Session Expiration17-09-20192.1A flaw was found in FreeIPA versions 4.5.0 and later. Session cookies were retained in the cache after logout. An attacker could abuse this flaw if they obtain previously valid session cookies and can use this to gain access to the session. CVE ID : CVE-2019-14826https://bug zilla.redhat. com/show. bug.cgi?id= (VF.2019- 14826geautomationEmerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX71 device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gila.cmsEmerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX71 device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gila.cmsEmerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX71 device. CVE ID : CVE-2019-16653N/AA-GEA-PROF- 141019/101gila.cmsEmerson GE III.11 allows admin/fm?f=./ directory traversal, leading to Local File Inclusion. CVE ID : CVE-2019-16679N/AA-GIL-GILA- 141019/102				CVE ID : CVE-2019-6145		
Insufficient Session Expiration17-09-20192.1A flaw was found in FreeIPA versions 4.5.0 and later. Session cookies were retained in the cache after logout. An attacker could abuse this flaw if they obtain previously valid session cookies and can use this to gain access to the session. CVE ID : CVE-2019-14826https://bug zilla.redhat. com/show_ bug.cgi?id= (VE-2019- 14826geautomation proficyEmerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX71 device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gilacmsImproper Limitation of a Pathname to a Restricted Directory (Path Traversal')Afila CMS before 1.11.1 allows admin/fm?f=./ directory traversal, leading to Local File Inclusion. CVE ID : CVE-2019-16679N/AA-GIL-GILA- 141019/102						
Insufficient Session ExpirationInsufficient Session cookies were retained in the cache after logout. An attacker could operviously valid session previously valid session cookies and can use this to gain access to the session. CVE ID : CVE-2019-14826A-FRE-FREE- 14009/100geautomationInterpret Session CVE ID : CVE-2019-14826A-FRE-FREE- stategeautomationInterpret Session (CVE-2019-14826A-FRE-FREE- stategeautomationInterpret Session (CVE-2019-14826A-FRE-FREE- stateImproper Input ValidationInterpret Input Session (CVE-2019-14826A-GEA-PROF- 14826glacmsInterpret Session (CVE-DI : CVE-2019-16353N/AA-GEA-PROF- 141019/101glacmsInterpret Session (CVE ID : CVE-2019-16353)Interpret Session (CVE ID : CVE-2019-16353)A-GEA-PROF- 141019/101Improper Session (CP ID : CVE-2019-16675)Interpret Session (CVE ID : CVE-2019-16675)Interpret Session (CVE ID : CVE-2019-16675)A-GEA-PROF- 141019/102Improper Session (CP ID : CVE-2019-16675)Interpret Session (CP ID : CVE-2019-16675)	freeipa					
ProficyImproper Input Validation16-09-20195Emerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gilacmsEmerson GE Automation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gilacmsEmerson GE Automation a Pathname to a Restricted Directory ('Path Traversal')A-GIL-GILA- 141019/102A-GIL-GILA- 141019/102		17-09-2019	2.1	versions 4.5.0 and later. Session cookies were retained in the cache after logout. An attacker could abuse this flaw if they obtain previously valid session cookies and can use this to gain access to the session.	zilla.redhat. com/show_ bug.cgi?id= CVE-2019-	
ProficyImproper Input Validation16-09-20195Emerson GE Automation Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gilacmsEmerson GE Automation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gilacmsEmerson GE Automation a Pathname to a Restricted Directory ('Path Traversal')A-GIL-GILA- 141019/102A-GIL-GILA- 141019/102	geautomation	1				
Improper Input Validation16-09-20195Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device. CVE ID : CVE-2019-16353N/AA-GEA-PROF- 141019/101gilacmsGila CMSgilacmsGila CMS before 1.11.1 allows admin/fm/?f=/ directory traversal, leading to Local File Inclusion. CVE ID : CVE-2019-16679N/AA-GEA-PROF- 141019/101	5					
gilacms gila_cms Jimproper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Handbox Hand	Improper Input Validation	16-09-2019	5	Proficy Machine Edition 8.0 allows an access violation and application crash via crafted traffic from a remote device, as demonstrated by an RX7i device.	N/A	
gila_cms Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') Gila CMS before 1.11.1 allows admin/fm/?f=/ directory traversal, leading to Local File Inclusion. CVE ID : CVE-2019-16679				CVE ID : CVE-2019-16353		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	-					
Limitation of a Pathname to a Restricted Directory ('Path Traversal')	0					Γ
Gitlab	Limitation of a Pathname to a Restricted Directory ('Path	21-09-2019	4	allows admin/fm/?f=/ directory traversal, leading to Local File Inclusion.	N/A	
	Gitlab	<u> </u>		· · · · · · · · · · · · · · · · · · ·	<u> </u>	<u> </u>

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				27						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
gitlab				1	
Incorrect Permission Assignment for Critical Resource	16-09-2019	5.5	An issue was discovered in GitLab Community and Enterprise Edition 10.8 through 12.2.1. An internal endpoint unintentionally allowed group maintainers to view and edit group runner settings. CVE ID : CVE-2019-15721	https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot- 3-released/	A-GIT-GITL- 141019/103
Uncontrolled Resource Consumption	16-09-20195GitLab Community and Enterprise Edition 8.15 through 12.2.1. Particular mathematical expressions in GitLab Markdown can exhaust client resources.ut.git m/20 y-relation dot-2			https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot- 3-released/	A-GIT-GITL- 141019/104
Incorrect Permission Assignment for Critical Resource	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 11.9.x and 11.10.x before 11.10.1. Merge requests created by email could be used to bypass push rules in certain situations. CVE ID : CVE-2019-15723	https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot- 3-released/	A-GIT-GITL- 141019/105
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	16-09-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition 11.10 through 12.2.1. Label descriptions are vulnerable to HTML injection. CVE ID : CVE-2019-15724	https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot- 3-released/	A-GIT-GITL- 141019/106
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 12.0	N/A	A-GIT-GITL- 141019/107
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 35	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			the ep result privat	gh 12.2. bic notes in discl ce milest ther info	API tha osure of ones, la	t could bels,				
			CVE I	D : CVE-	2019-1	5725				
Information Exposure	16-09-2019	5	GitLab Community and Enterprise Edition through 12.2.1. Embedded images and media files in markdown could be pointed to an arbitrary server, which would reveal the IP address of clients requesting the file from that server. CVE ID : CVE-2019-15726 An issue was discovered in CitLab Community and				https:, ut.gitla m/201 /29/se y-relea gitlab- dot-2- 3-relea	ab.co 19/08 ecurit ase- 12- dot-	A-GIT-0 141019	
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 11.2 through 12.2.1. Insufficient permission checks were being applied when displaying CI results, potentially exposing some CI metrics data to unauthorized users. CVE ID : CVE-2019-15727				https:/ ut.gitla m/201 /29/se y-relea gitlab- dot-2- 3-relea	ab.co 19/08 ecurit ase- 12- dot-	A-GIT-0 141019	
Server-Side Request Forgery (SSRF)	16-09-2019	5	CVE ID : CVE-2019-15727 An issue was discovered in GitLab Community and Enterprise Edition 10.1 through 12.2.1. Protections against SSRF attacks on the Kubernetes integration are insufficient, which could have allowed an attacker to request any local network resource accessible from the GitLab server.				N/A		A-GIT-0 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	ch	NCIIP	CID
			CVE ID	: CVE-	2019-1	5728				
Information Exposure	17-09-2019	5	An issue GitLab (Enterpr through endpoin disclose the last a merge CVE ID	Communise Ed n 12.2 nt unim ed info pipelime e reque	unity an ition 8.1 1. An inf tention rmation ne that p est.	nd 18 ternal ally n about ran for	N/A		A-GIT-G 141019	
Server-Side Request Forgery (SSRF)	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 8.14 through 12.2.1. The Jira integration contains a SSRF vulnerability as a result of a bypass of the current protection mechanisms against this type of attack, which would allow sending requests to any resources accessible in the local network by the GitLab server.			N/A		A-GIT-G 141019		
Incorrect Permission Assignment for Critical Resource	16-09-2019	5	An issue GitLab (Enterpr through membe comme despite set to al membe CVE ID	Communise Ed n 12.2.1 ers wer nt on r the re llow or ers to d	unity an ition 12 1. Non- e able to nerge ro pository nly projo o so.	nd 2.0 o equests y being ect	https:, ut.gitla m/202 /29/so y-relea gitlab- dot-2- 3-relea	ab.co 19/08 ecurit ase- 12- dot-	A-GIT-G 141019	
Information Exposure	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition 12.2 through 12.2.1. The project			https://abo ut.gitlab.co m/2019/08 /29/securit		A-GIT-GITL- 141019/114		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			import API could be used to bypass project visibility restrictions. CVE ID : CVE-2019-15732	y-release- gitlab-12- dot-2-dot- 3-released/	
Information Exposure	16-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 7.12 through 12.2.1. The specified default branch name could be exposed to unauthorized users. CVE ID : CVE-2019-15733	https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot- 3-released/	A-GIT-GITL- 141019/115
Information Exposure	16-09-2019	4	An issue was discovered in GitLab Community and Enterprise Edition 8.6 through 12.2.1. Under very specific conditions, commit titles and team member comments could become viewable to users who did not have permission to access these.	https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot- 3-released/	A-GIT-GITL- 141019/116
			CVE ID : CVE-2019-15734		
Uncontrolled Resource Consumption	16-09-2019	5	An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Under certain circumstances, CI pipelines could potentially be used in a denial of service attack. CVE ID : CVE-2019-15736	https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot- 3-released/	A-GIT-GITL- 141019/117
Improper Authenticati on	16-09-2019	6.4	An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Certain account actions needed improved authentication and session management.	https://abo ut.gitlab.co m/2019/08 /29/securit y-release- gitlab-12- dot-2-dot-	A-GIT-GITL- 141019/118

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
20										

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIF	PC ID
			CVE I	D : CVE-	2019-1	5737	3-rele	ased/		
Information Exposure	16-09-2019	5	GitLak Entery throug certai reque disclo	An issue was discovered in GitLab Community and Enterprise Edition 12.0 through 12.2.1. Under certain conditions, merge request IDs were being disclosed via email. CVE ID : CVE-2019-15738 An issue was discovered in				//abo ab.co 19/08 ecurit ase- ·12- dot- ased/	A-GIT-0 141019	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	16-09-2019	4.3	GitLak Entery throug displa not pr XSS pa	ue was o o Comm prise Ed gh 12.2. ying Ma operly s ayloads. D : CVE-	unity an ition 8.1 1. Certai rkdown anitizin	in areas in were ig some	https:, ut.gitl m/20 /29/s y-relea gitlab- dot-2- 3-rele	ab.co 19/08 ecurit ase- 12- dot-	A-GIT-0 141019	
Information Exposure	16-09-2019	5	GitLak Entery throug Geolo being image	ue was o o Comm prise Ed gh 12.2. cation d remove upload D : CVE-	unity an ition 7.9 1. EXIF ata was d from o s.	not certain	N/A		A-GIT-0 141019	
Incorrect Permission Assignment for Critical Resource	16-09-2019	5.5	GitLal 11.x a 12.1.x 12.2.x Incorr	ue was o 5 Enterp nd 12.x before before cect Acco D : CVE-	rise Edi before 1 12.1.9, a 12.2.5. I ess Cont	tion 2.0.9, and t has crol.	N/A		A-GIT-0 141019	
gnucobol_project										
gnucobol										
Buffer Copy without Checking Size of Input	17-09-2019	6.8	GnuCOBOL 2.2 has a stack- based buffer overflow in the cb_name() function in cobc/tree.c via crafted		N/A		A-GNU- 141019			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	l	Description	on & CVE	ID	Pat	tch	NCIIP	C ID
('Classic Buffer Overflow')				L source D : CVE ·		6395				
Use After Free	17-09-2019	6.8	after- end_s e() fur via cr code.	OBOL 2. free in t cope_of nction in afted CC D : CVE ·	he _progran 1 cobc/r 1BOL sou	n_nam parser.y urce	N/A		A-GNU- 141019	
Gradle										
gradle										
Improper Input Validation	16-09-2019	4.3	Gradl the SF might replac differ same a rela 4900.	GP signi e before HA-1 alg allow a ce an art ent one SHA-1 r ted issue D : CVE -	6.0 relia orithm, n attack ifact with that has nessage e to CVE	es on which er to th a the digest, -2005-	N/A		A-GRA- 141019	
grafana			•							
grafana										
Insufficiently Protected Credentials	23-09-2019	4	An issue was discovered in Grafana 5.4.0. Passwords for data sources used by Grafana (e.g., MySQL) are not encrypted. An admin user can reveal passwords for any data source by pressing the "Save and test" button within a data source's settings menu. When watching the transaction with Burp Proxy, the password for the data source is revealed and sent to the			N/A		A-GRA-0 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server. From a browser, a prompt to save the credentials is generated, and the password can be revealed by simply checking the "Show password" box. CVE ID : CVE-2019-15635		
halo					
halo					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Halo 1.1.0 has XSS via a crafted authorUrl in JSON data to api/content/posts/comment s. CVE ID : CVE-2019-16890	N/A	A-HAL-HALO- 141019/127
Haxx					
curl					
Double Free	16-09-2019	7.5	Double-free vulnerability in the FTP-kerberos code in cURL 7.52.0 to 7.65.3. CVE ID : CVE-2019-5481	N/A	A-HAX-CURL- 141019/128
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-09-2019	7.5	Heap buffer overflow in the TFTP protocol handler in cURL 7.19.4 to 7.65.3. CVE ID : CVE-2019-5482	N/A	A-HAX-CURL- 141019/129
hcltech					
appscan_sour	ce				
Improper Restriction of XML External Entity	25-09-2019	5.8	HCL AppScan Source before 9.03.13 is susceptible to XML External Entity (XXE) attacks in multiple locations. In particular, an attacker can	https://hcl pnpsupport. hcltech.com /csm?id=kb _article&sys	A-HCL-APPS- 141019/130
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
Reference ('XXE')			send a specially crafted .ozasmt file to a targeted victim and ask the victim to open it. When the victim imports the .ozasmt file in AppScan Source, the content of any file in the local file system (to which the victim as read access) can be exfiltrated to a remote listener under the attacker's control. The product does not disable external XML Entity Processing, which can lead to information disclosure and denial of services attacks. CVE ID : CVE-2019-16188			_id=08 961b0 07776 d4bcb	c885 1fc58			
hongcms_pro	iect		CVEI	D : CVE-	2019-1	6188				
hongcms										
Improper Input Validation	25-09-2019	5.5	arbitr / in t admin ajax?a issue the at config instal reinst	CMS 3.0. ary file of the file p n/index.j action=d to CVE-2 tacker d g.php and l/index.j tall the p D : CVE-	deletion aramete php/dat elete, a s 2018-16 eletes d visits php, the roduct.)	via a er to abase/ similar 774. (If y can	N/A		A-HON- HONG- 141019	/131
hrworks										
hrworks				. 10						
Improper Neutralizatio n of Input During Web Page Generation	17-09-2019	4.3	A reflected Cross-site scripting (XSS) vulnerability in HRworks V 1.16.1 allows remote attackers to inject arbitrary web script or HTML via the URL				N/A		A-HRW- HRWO- 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
('Cross-site Scripting')			-	neter to onent.	the Log	in				
			CVE I	D : CVE-	2019-1	1559				
html-pdf_proj	ject						<u> </u>		<u> </u>	
html-pdf										
Information Exposure	20-09-2019	5	for N file re HTM XML file://	itml-pdf ode.js ha ead vulne L file tha IttpRequ // URL.	s an arb erability t uses iest to a	itrary via an ccess a	N/A		A-HTM- HTML- 141019	
			CVE I	D : CVE-	2019-1	5138				
hunspell_proj	ject									
hunspell			1				T		T	
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-09-2019	4.3	read Sugge string	pell 1.7.0 operatio estMgr::l g in sugg (D : CVE-	n in eftcomr estmgr.(nonsub cxx.	N/A		A-HUN- 141019	
IBM	I						<u>. </u>			
cognos_analy	tics									
Uncontrolled Resource Consumption	17-09-2019	7.8	IBM Cognos Analytics 11.0, and 11.1 is vulnerable to a denial of service attack that could allow a remote user to send specially crafted requests that would consume all available CPU and memory resources. IBM X-Force ID: 158973. CVE ID : CVE-2019-4183			https:, w.ibm suppo ges/nd 07353	.com/ rt/pa ode/1 0	A-IBM-0 141019	/135	
Improper Neutralizatio n of Input	17-09-2019	3.5	IBM Cognos Analytics 11.0 and 11.1 is vulnerable to cross-site scripting. This			https: w.ibm suppo	.com/	A-IBM-0 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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: 161421. CVE ID : CVE-2019-4342	ges/node/1 073530	
mq	I			I	I
Improper Input Validation	26-09-2019	4	IBM MQ 7.5.0.0 - 7.5.0.9, 7.1.0.0 - 7.1.0.9, 8.0.0.0 - 8.0.0.12, 9.0.0.0 - 9.0.0.6, 9.1.0.0 - 9.1.0.2, and 9.1.0 - 9.1.2 command server is vulnerable to a denial of service attack caused by an authenticated and authorized user using specially crafted PCF messages. IBM X-Force ID: 162084. CVE ID : CVE-2019-4378	https://sup portcontent .ibm.com/s upport/pag es/node/88 6885	A-IBM-MQ- 141019/137
application_p	erformance_r	nanage			
Improper Restriction of Rendered UI Layers or Frames	17-09-2019	4.3	IBM Cloud Application Performance Management 8.1.4 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: 157509.	https://ww w.ibm.com/ support/pa ges/securit y-bulletin- ibm- application- performanc e- managemen t-could- allow- remote- attacker-	A-IBM-APPL- 141019/138
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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-2019-4086	hijack- clicking- action- victim-cve- 2019-4086	
cognos_contro	oller				
Inadequate Encryption Strength	17-09-2019	5	IBM Cognos Controller 10.3.0, 10.3.1, 10.4.0, and 10.4.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X- Force ID: 158880. CVE ID : CVE-2019-4175	https://ww w.ibm.com/ support/pa ges/securit y-bulletin- security- vulnerabilti es-exist- ibm- cognos- controller	A-IBM-COGN- 141019/139
Information Exposure	17-09-2019	4.3	IBM Cognos Controller 10.3.0, 10.3.1, 10.4.0, and 10.4.1 does not set the secure attribute on authorization tokens or session cookies. This could allow an attacker to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 158876. CVE ID : CVE-2019-4171	https://ww w.ibm.com/ support/pa ges/securit y-bulletin- security- vulnerabilti es-exist- ibm- cognos- controller	A-IBM-COGN- 141019/140
sterling_file_g	ateway				
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	16-09-2019	6.5	IBM Sterling File Gateway 2.2.0.0 through 6.0.1.0 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end	https://ww w.ibm.com/ support/pa ges/securit y-bulletin- sql- injection- vulnerabilit y-affects-	A-IBM-STER- 141019/141
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			database. IBM X-Force ID: 158413. CVE ID : CVE-2019-4147	ibm- sterling- file- gateway- cve-2019- 4147	
security_key_	lifecycle_man	ager			
Cross-Site Request Forgery (CSRF)	24-09-2019	4.3	IBM Security Key Lifecycle Manager 3.0 and 3.0.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 165137. CVE ID : CVE-2019-4515	https://ww w.ibm.com/ support/pa ges/node/2 90671	A-IBM-SECU- 141019/142
Weak Password Requirement s	20-09-2019	5	IBM Security Key Lifecycle Manager 3.0 and 3.0.1 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 166626. CVE ID : CVE-2019-4565	https://ww w.ibm.com/ support/pa ges/securit y-bulletin- ibm- security- key- lifecycle- manager- uses-weak- password- policy-cve- 2019-4565	A-IBM-SECU- 141019/143
Cleartext Storage of Sensitive Information	24-09-2019	2.1	IBM Security Key Lifecycle Manager 3.0 and 3.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 166627. CVE ID : CVE-2019-4566	https://ww w.ibm.com/ support/pa ges/node/1 074344	A-IBM-SECU- 141019/144
websphere_ap		ver			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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	17-09-2019	4	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a user with access to audit logs to obtain sensitive information, caused by improper handling of command line options. IBM X-Force ID: 163997. CVE ID : CVE-2019-4477	https://ww w.ibm.com/ support/pa ges/node/9 60290	A-IBM-WEBS- 141019/145
Information Exposure	20-09-2019	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Network Deployment could allow a remote attacker to obtain sensitive information, caused by sending a specially-crafted URL. This can lead the attacker to view any file in a certain directory. IBM X-Force ID: 164364. CVE ID : CVE-2019-4505	https://ww w.ibm.com/ support/pa ges/node/9 64766	A-IBM-WEBS- 141019/146
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-09-2019	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL containing "dot dot" sequences (//) to view arbitrary files on the system. IBM X-Force ID: 160201. CVE ID : CVE-2019-4268	https://ww w.ibm.com/ support/pa ges/node/8 84030	A-IBM-WEBS- 141019/147
Improper Neutralizatio n of Input During Web Page	17-09-2019	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console is vulnerable to cross-site scripting. This vulnerability allows users to	https://ww w.ibm.com/ support/pa ges/node/8 84036	A-IBM-WEBS- 141019/148
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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')			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: 160203.		
			CVE ID : CVE-2019-4270		
Improper Input Validation	17-09-2019	3.5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin console is vulnerable to a Client-side HTTP parameter pollution vulnerability. IBM X-Force ID: 160243. CVE ID : CVE-2019-4271	https://ww w.ibm.com/ support/pa ges/node/8 84040	A-IBM-WEBS- 141019/149
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-09-2019	4	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9,0 could allow a remote attacker to traverse directories on the file system. An attacker could send a specially-crafted URL request to view arbitrary files on the system but not content. IBM X-Force ID: 163226. CVE ID : CVE-2019-4442	https://ww w.ibm.com/ support/pa ges/node/9 59021	A-IBM-WEBS- 141019/150
websphere_vi	irtual enterpi	rise			
Information Exposure	20-09-2019	5	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Network Deployment could allow a remote attacker to obtain sensitive information, caused by sending a specially-crafted URL. This can lead the attacker to view any file in a certain	https://ww w.ibm.com/ support/pa ges/node/9 64766	A-IBM-WEBS- 141019/151
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Improper Neutralizatio n of Input During Web Page Generation (Cross-site Scripting')25-09-2019 25-09-2019IBM Content Navigator 3.0CD 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: 166721. CVE D1 : CVE-2019-4571A-IBM-CONT- 141019/152qradar_security_information_autevent_managerIBM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF)Itps://ww wulbm.com/ support/pa ges/node/1 073576A-IBM-QRAD- 141019/152Server-Side Request Forgery (SSRF)26-09-20195IBM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. (VF ID : CVE-2019-4E671https://ww wulbm.com/ sendunauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. (VF ID : CVE-2019-4E671N/AA-IBR-ORAD- 141019/153idreamsoft (CSSF)21-09-20195.8An issue was discovered in idreamsoft iCMS V7.0. adminep.php?app=members &do-del allows CSRF. CVE ID : CVE-2019-16677N/AA-IDR-ICMS- A1019/154	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
CVE ID : CVE-2019-4505content_navigatorCVE ID : CVE-2019-4505content_navigatorImproper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')25-09-20193.5IBM Content Navigator 3.0CD is vulnerable to cross- site scripting. This vulnerability allows users to embed arbitrary JavaScriptic ode in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 1.66721.https://ww wulm.com/ support/pa ges/node/1A-IBM-CONT- ful1019/152Greatar_security_information to vertent_mangerIBM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 1.60014. CVE ID : CVE-2019-4262https://ww wulm.com/ support/pa ges/node/1A-IBM-QRAD- 141019/153foreases/ite21-09-20195.8An issue was discovered in idreamsoft iCMS V7.0. adminep.php?apn=members &do-del allows CSRF. CVE ID : CVE-2019-16677N/AA-IDR-ICMS- 141019/154				•							
content_navigatorcontent_navigatorImproper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')1BM Content Navigator 3.0CD 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: 166721. CVE ID : CVE-2019-4571https://ww w.ibm.com/ support/pa ges/node/1 073576A-IBM-CONT- 141019/152gradar_security_information_weight Server-Side Request Forgery (SSRF)BM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. CVE ID : CVE-2019-4262https://ww w.ibm.com/ support/pa ges/node/1A-IBM-QRAD- 141019/153Cross-Site Request ForgeryCross-Site Request ForgeryCross-Site Request Forgery21-09-20195.8An issue was discovered in idreamsoft iCMS V7.0. admincp.php?app=members &do=del allows CSRF. CVE ID : CVE-2019-16677N/AA-IDR-ICMS- 141019/154											
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')25-09-20193.5IBM Content Navigator 3.0CD 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: 166721.https://ww w.ibm.com/ support/pa ges/node/1A-IBM-CONT- 141019/152 qradar_security_informatio_rand_event_manager IBM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthentized datacker to send unauthentized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. CVE ID: CVE-2019-4262https://ww w.ibm.com/ support/pa ges/node/1A-IBM-QRAD- 141019/153Gross-Site Request Forgery (SSRF)21-09-20195.8An issue was discovered in idreamsoft iCMS V7.0. adminc.php?app=members &do=del allows CSRF. CVE ID: CVE-2019-16677N/AA-IDR-ICMS- 141019/153	contont novi	rator		CVE ID : CVE-2019-4505							
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')3.53.0CD is vulnerable to cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript hattering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 166721. CVE ID: CVE-2019-4571https://ww w.ibm.com/ support/pa ges/node/1A-IBM-CONT- 141019/152gradar_security_information regres Server-Side Request Forgery (SSRF)26-09-20195IBM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. CVE ID: CVE-2019-4262A-IBM-QRAD- 141019/153Cross-Site Request Forgery (CSRF)21-09-20195.8An issue was discovered in idreamsoft iCMS V7.0. admincp.ph?app=members &do=del allows CSRF. CVE ID: CVE-2019-16677N/AA-IDR-ICMS- 141019/154	content_navi										
Server-Side Request Forgery (SSRF)26-09-20195IBM QRadar SIEM 7.2 and 7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. CVE ID : CVE-2019-4262https://ww w.ibm.com/ support/pa ges/node/1 074538A-IBM-QRAD- 141019/153icms	Neutralizatio n of Input During Web Page Generation ('Cross-site	25-09-2019	3.5	3.0CD 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: 166721.	w.ibm.com/ support/pa ges/node/1						
Server-Side Request Forgery (SSRF)26-09-201957.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014. CVE ID : CVE-2019-4262https://ww wibm.com/ support/pa ges/node/1A-IBM-QRAD- 141019/153dreamsoftImage: CV Scoring ScaleImage: CV Scoring ScaleAn issue was discovered in idreamsoft iCMS V7.0. admincp.php?app=members &do=del allows CSRF. CVE ID : CVE-2019-16677N/AA-IDR-ICMS- 141019/154	qradar_security_information_and_event_manager										
icms Cross-Site An issue was discovered in Request 21-09-2019 Forgery 5.8 An issue was discovered in idreamsoft iCMS V7.0. admincp.php?app=members &do=del allows CSRF. CV Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Request Forgery	26-09-2019	5	7.3 is vulnerable to Server Side Request Forgery (SSRF). This may allow an unauthenticated attacker to send unauthorized requests from the QRadar system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 160014.	w.ibm.com/ support/pa ges/node/1	e					
Cross-Site Request Forgery (CSRF) 21-09-2019 5.8 An issue was discovered in idreamsoft iCMS V7.0. admincp.php?app=members &do=del allows CSRF. N/A A-IDR-ICMS- 141019/154 CV Scoring Scale 0.1 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.9 9.10	idreamsoft	<u> </u>									
Cross-Site Request Forgery (CSRF) 21-09-2019 5.8 idreamsoft iCMS V7.0. admincp.php?app=members &do=del allows CSRF. N/A A-IDR-ICMS- 141019/154 CV Scoring Scale 0.1 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.9 9.10	icms										
	Request Forgery	21-09-2019	5.8	idreamsoft iCMS V7.0. admincp.php?app=members &do=del allows CSRF.	N/A						
	-										

Weakness	Publish Date	CVSS	Description & C	/E ID	Pate	ch	NCIIF	PC ID
Imagemagick		•						
imagemagick								
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8- memory leak in coders/dot.c, as demonstrated by AcquireMagickMem MagickCore/memor	ory in ry.c.	N/A		A-IMA-1 141019	
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8- memory leak in Huffman2DEncodeI coders/ps2.c. CVE ID : CVE-2019	N/A		A-IMA-1 141019		
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8- memory leak in Huffman2DEncodel coders/ps3.c, as demonstrated by WritePS3Image. CVE ID : CVE-2019	N/A		A-IMA- 141019		
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8- memory leak in coders/dot.c, as demonstrated by Pi in MagickCore/cons CVE ID : CVE-2019	ngImage stitute.c.	N/A		A-IMA-1 141019	
Missing Release of Resource after Effective Lifetime	23-09-2019	4.3	ImageMagick 7.0.8- memory leak in magick/xwindow.c, to XCreateImage. CVE ID : CVE-2019	related	N/A		A-IMA-IMAG- 141019/159	
Missing Release of Resource after	23-09-2019	4.3	ImageMagick 7.0.8- memory leak in coders/dps.c, as demonstrated by	35 has a	N/A		A-IMA-1 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2 -3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Effective			XCreateImage.		
Lifetime			CVE ID : CVE-2019-16709		
Infradead					
openconnect					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.5	process_http_response in OpenConnect before 8.05 has a Buffer Overflow when a malicious server uses HTTP chunked encoding with crafted chunk sizes. CVE ID : CVE-2019-16239	N/A	A-INF-OPEN- 141019/161
inoideas	L				
inoerp					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	26-09-2019	7.5	download.php in inoERP 4.15 allows SQL injection through insecure deserialization. CVE ID : CVE-2019-16894	N/A	A-INO-INOE- 141019/162
integard_pro_	project				•
integard_pro					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-09-2019	7.5	Integard Pro 2.2.0.9026 allows remote attackers to execute arbitrary code via a buffer overflow involving a long NoJs parameter to the /LoginAdmin URI. CVE ID : CVE-2019-16702	N/A	A-INT-INTE- 141019/163
Intel					
easy_streamin	ng_wizard				
Improper Privilege Management	16-09-2019	4.6	Improper file permissions in the installer for Intel(R) Easy Streaming Wizard before	https://ww w.intel.com /content/w	A-INT-EASY- 141019/164
CV Scoring Scale	0	1-2			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			version 2.1.0731 may allow an authenticated user to potentially enable escalation of privilege via local attack. CVE ID : CVE-2019-11166	ww/us/en/ security- center/advi sory/intel- sa- 00285.html						
Ipswitch										
moveit_transfer										
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	24-09-2019	 MOVEit.DMZ.WebApi.dll in Progress MOVEit Transfer 2018 SP2 before 10.2.4, 2019 before 11.0.2, and 2019.1 before 11.1.1 allows an unauthenticated attacker to gain unauthorized access to the database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may be able to infer information about the structure and contents of the database, or may be able to alter the database via the REST API, aka SQL Injection. CVE ID : CVE-2019-16383 		https://doc s.ipswitch.c om/MOVEit /Transfer2 019_1/Rele aseNotes/e n/index.ht m#49443.h tm	A-IPS-MOVE- 141019/165					
Irfanview										
irfanview										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	25-09-2019	6.8	In IrfanView 4.53, Data from a Faulting Address controls a subsequent Write Address starting at image00400000+0x000000 000001dcfc. CVE ID : CVE-2019-16887	N/A	A-IRF-IRFA- 141019/166					
Jenkins										
aqua_security_scanner										

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
E2										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmissio n of Sensitive Information	25-09-2019	5	Jenkins Aqua Security Scanner Plugin 3.0.17 and earlier transmitted configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. CVE ID : CVE-2019-10428	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1508	A-JEN-AQUA- 141019/167
jenkins					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:expandableTextBox form control interpreted its content as HTML when expanded, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents (typically Job/Configure). CVE ID : CVE-2019-10401	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1498	A-JEN-JENK- 141019/168
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:combobox form control interpreted its item labels as HTML, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents. CVE ID : CVE-2019-10402	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1525	A-JEN-JENK- 141019/169
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the SCM tag name on the tooltip for SCM tag actions, resulting in a stored XSS vulnerability exploitable by users able to control SCM tag names for these actions.	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY- 1537%20(1)	A-JEN-JENK- 141019/170
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-10403		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the reason why a queue items is blcoked in tooltips, resulting in a stored XSS vulnerability exploitable by users able to control parts of the reason a queue item is blocked, such as label expressions not matching any idle executors. CVE ID : CVE-2019-10404	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY- 1537%20(2)	A-JEN-JENK- 141019/171
Information Exposure	25-09-2019	4	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier printed the value of the "Cookie" HTTP request header on the /whoAmI/ URL, allowing attackers exploiting another XSS vulnerability to obtain the HTTP session cookie despite it being marked HttpOnly. CVE ID : CVE-2019-10405	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1505	A-JEN-JENK- 141019/172
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not restrict or filter values set as Jenkins URL in the global configuration, resulting in a stored XSS vulnerability exploitable by attackers with Overall/Administer permission. CVE ID : CVE-2019-10406	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1471	A-JEN-JENK- 141019/173
inheritance-p	lugin		L		
Information Exposure	25-09-2019	4	Jenkins Project Inheritance Plugin 2.0.0 and earlier displayed a list of	https://jen kins.io/secu rity/advisor	A-JEN-INHE- 141019/174
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			environment variables passed to a build without masking sensitive variables contributed by the Mask Passwords Plugin.	y/2019-09- 25/#SECUR ITY-351					
			CVE ID : CVE-2019-10407						
project_inher	itance			<u> </u>					
Incorrect Authorizatio n	25-09-2019	4	A cross-site request forgery vulnerability in Jenkins Project Inheritance Plugin 2.0.0 and earlier allowed attackers to trigger project generation from templates. CVE ID : CVE-2019-10408	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-401	A-JEN-PROJ- 141019/175				
log_parser									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	25-09-2019	3.5	Jenkins Log Parser Plugin 2.0 and earlier did not escape an error message, resulting in a cross-site scripting vulnerability exploitable by users able to define log parsing rules. CVE ID : CVE-2019-10410	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-732	A-JEN-LOG 141019/176				
inedo_buildm	aster			I					
Cleartext Transmissio n of Sensitive Information	25-09-2019	5	Jenkins Inedo BuildMaster Plugin 2.4.0 and earlier transmitted configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. CVE ID : CVE-2019-10411	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1513	A-JEN-INED- 141019/177				
inedo_proget									
Cleartext Transmissio n of Sensitive	25-09-2019	5	Jenkins Inedo ProGet Plugin 1.2 and earlier transmitted configured credentials in	https://jen kins.io/secu rity/advisor	A-JEN-INED- 141019/178				
CV Scoring Scal	ρ				8.0 0.10				

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				55						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Information			plain text as part of the global Jenkins configuration form, potentially resulting in their exposure.	y/2019-09- 25/#SECUR ITY-1514					
			CVE ID : CVE-2019-10412						
data_theorem	_mobile_app_	securi	ty						
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Data Theorem: CI/CD Plugin 1.3 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system. CVE ID : CVE-2019-10413	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1557	A-JEN-DATA- 141019/179				
git_changelog									
Cleartext Storage of Sensitive Information	25-09-2019	3.5	Jenkins Git Changelog Plugin 2.17 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system.	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1574	A-JEN-GIT 141019/180				
			CVE ID : CVE-2019-10414						
violation_com	iments_to_git	lab							
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Violation Comments to GitLab Plugin 2.28 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system.	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1577	A-JEN-VIOL- 141019/181				
CV Scoring Scal (CVSS)	CV Scoring Scale (CVSS) 0-1 1-2 2-3 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-2019-10415						
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Violation Comments to GitLab Plugin 2.28 and earlier stored credentials unencrypted in job config.xml files on the Jenkins master where they could be viewed by users with Extended Read permission, or access to the master file system. CVE ID : CVE-2019-10416	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1577	A-JEN-VIOL- 141019/182				
kubernetes_pipeline									
Improper Privilege Management	25-09-2019	6.5	Jenkins Kubernetes :: Pipeline :: Kubernetes Steps Plugin provides a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection. CVE ID : CVE-2019-10417	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY- 920%20(1)	A-JEN-KUBE- 141019/183				
Improper Privilege Management	25-09-2019	6.5	Jenkins Kubernetes :: Pipeline :: Arquillian Steps Plugin provides a custom whitelist for script security that allowed attackers to invoke arbitrary methods, bypassing typical sandbox protection. CVE ID : CVE-2019-10418	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY- 920%20(2)	A-JEN-KUBE- 141019/184				
vfabric_appli	cation_directo	or							
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins vFabric Application Director Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR TIY-1541	A-JEN-VFAB- 141019/185				
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			with access to the master file system. CVE ID : CVE-2019-10419			
assembla	I					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins Assembla Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. CVE ID : CVE-2019-10420	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1543	A-JEN-ASSE- 141019/186	
azure_event_g	grid_notifier					
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Azure Event Grid Build Notifier Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. CVE ID : CVE-2019-10421	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1544	A-JEN-AZUR- 141019/187	
call_remote_j	ob					
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Call Remote Job Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. CVE ID : CVE-2019-10422	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1548	A-JEN-CALL- 141019/188	
codescan	I					
Cleartext	25-09-2019	2.1	Jenkins CodeScan Plugin	https://jen	A-JEN-CODE-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Storage of Sensitive Information			stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. CVE ID : CVE-2019-10423	kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1551	141019/189
eloyente					
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins elOyente Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. CVE ID : CVE-2019-10424	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1561	A-JEN-ELOY- 141019/190
google_calend	lar				
Cleartext Storage of Sensitive Information	25-09-2019	4	Jenkins Google Calendar Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. CVE ID : CVE-2019-10425	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1572	A-JEN-GOOG- 141019/191
gem_publishe	er				
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins Gem Publisher Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1573	A-JEN-GEM 141019/192
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-10426			
gitlab_logo	I			<u> </u>	I	
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins GitLab Logo Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. CVE ID : CVE-2019-10429	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1575	A-JEN-GITL- 141019/193	
neuvector_vu	lnerability_sc	anner				
Cleartext Storage of Sensitive Information	25-09-2019	2.1	Jenkins NeuVector Vulnerability Scanner Plugin 1.5 and earlier stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system. CVE ID : CVE-2019-10430	https://jen kins.io/secu rity/advisor y/2019-09- 25/#SECUR ITY-1504	A-JEN-NEUV- 141019/194	
aqua_microsc	anner					
Cleartext Transmissio n of Sensitive Information	25-09-2019	5	Jenkins Aqua MicroScanner Plugin 1.0.7 and earlier transmitted configured credentials in plain text as part of the global Jenkins configuration form, potentially resulting in their exposure. CVE ID : CVE-2019-10427		A-JEN-AQUA- 141019/195	
Joomla				<u> </u>	<u> </u>	
joomla!						
Improper Neutralizatio n of Input	24-09-2019	4.3	In Joomla! 3.x before 3.9.12, inadequate escaping allowed XSS attacks using the logo	https://dev eloper.joom la.org/secur	A-JOO-JOOM- 141019/196	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
During Web Page Generation ('Cross-site Scripting')			parameter of the default templates. CVE ID : CVE-2019-16725	ity- centre/791- 20190901- core-xss-in- logo- parameter- of-default- templates.h tml		
joyplus_proje	ct					
joyplus						
Improper Input Validation	21-09-2019	6.4	joyplus-cms 1.6.0 allows reinstallation if the install/ URI remains available. CVE ID : CVE-2019-16655	N/A	A-JOY-JOYP- 141019/197	
Improper Input Validation	21-09-2019	7.5	joyplus-cms 1.6.0 allows remote attackers to execute arbitrary PHP code via /install by placing the code in the name of an object in the database. CVE ID : CVE-2019-16656	N/A	A-JOY-JOYP- 141019/198	
Cross-Site Request Forgery (CSRF)	21-09-2019	6.8	joyplus-cms 1.6.0 has admin_ajax.php?action=save xml&tab=vodplay CSRF. CVE ID : CVE-2019-16660	N/A	A-JOY-JOYP- 141019/199	
kkcms_projec	t					
kkcms						
Cross-Site Request Forgery (CSRF)	23-09-2019	6.8	kkcms v1.3 has a CSRF vulnerablity that can add an user account via admin/cms_user_add.php. CVE ID : CVE-2019-16706	N/A	A-KKC-KKCM- 141019/200	
Improper Neutralizatio n of Input During Web	27-09-2019	4.3	kkcms 1.3 has jx.php?url= XSS. CVE ID : CVE-2019-16923	N/A	A-KKC-KKCM- 141019/201	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Page Generation ('Cross-site Scripting')						
layerbb	I					
layerbb						
Cross-Site Request Forgery (CSRF)	19-09-2019	6.8	LayerBB before 1.1.4 has multiple CSRF issues, as demonstrated by changing the System Settings via admin/general.php. CVE ID : CVE-2019-16531	N/A	A-LAY-LAYE- 141019/202	
Lenovo						
system_upda	te					
Improper Input Validation	26-09-2019	7.8	A denial of service vulnerability was reported in Lenovo System Update versions prior to 5.07.0088 that could allow configuration files to be written to non-standard locations. CVE ID : CVE-2019-6175	N/A	A-LEN-SYST- 141019/203	
Libav						
libav						
Improper Input Validation	19-09-2019	7.1	In Libav 12.3, a denial of service in the subtitle decoder allows attackers to hog the CPU via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c has a complex format argument to sscanf. CVE ID : CVE-2019-9717		A-LIB-LIBA- 141019/204	
Buffer Copy without	19-09-2019	6.8	A stack-based buffer overflow in the subtitle	N/A	A-LIB-LIBA- 141019/205	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			decoder in Libav 12.3 allows attackers to corrupt the stack via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c misuses snprintf.		
			CVE ID : CVE-2019-9719		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	19-09-2019	7.1	A stack-based buffer overflow in the subtitle decoder in Libav 12.3 allows attackers to corrupt the stack via a crafted video file in Matroska format, because srt_to_ass in libavcodec/srtdec.c misuses snprintf.	N/A	A-LIB-LIBA- 141019/206
			CVE ID : CVE-2019-9720		
libgcrypt20_p	oroject				
libgcrypt20					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	25-09-2019	6.8	It was discovered that there was a ECDSA timing attack in the libgcrypt20 cryptographic library. Version affected: 1.8.4-5, 1.7.6-2+deb9u3, and 1.6.3- 2+deb8u4. Versions fixed: 1.8.5-2 and 1.6.3-2+deb8u7. CVE ID : CVE-2019-13627	N/A	A-LIB-LIBG- 141019/207
Libming					
libming					
Out-of- bounds Read	23-09-2019	6.4	Ming (aka libming) 0.4.8 has an out of bounds read vulnerability in the function OpCode() in the decompile.c file in libutil.a. CVE ID : CVE-2019-16705	N/A	A-LIB-LIBM- 141019/208
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pa	tch	NCIIF	C ID
libwav_projec	ct	<u> </u>	<u> </u>				<u> </u>		<u> </u>	
libwav										
NULL Pointer Dereference	16-09-2019	4.3	2019 point gain_f	•q libway •08-15 h er derefe file() at v D : CVE-	as a NU erence in vav_gain	LL 1 1.c.	N/A		A-LIB-L 141019	
linea_project	L		1				L		I	
linea										
Double Free	25-09-2019	7.5	the lin for Ru in the metho	sue was o nea crate 1st. Ther Matrix:: od. D : CVE-	e throug e is dou zip_eler	h 0.9.4 ble free nents	https: sec.or isorie: TSEC- 0021.	s/RUS 2019-	A-LIN-I 141019	
Linecorp										
line										
Integer Overflow or Wraparound	19-09-2019	6.8	Integer overflow vulnerability in LINE(Android) from 4.4.0 to the version before 9.15.1 allows remote attackers to cause a denial of service (DoS) condition or execute arbitrary code via a specially crafted image. CVE ID : CVE-2019-6010			N/A		A-LIN-I 141019		
Linuxfoundat	ion									
runc										
Incorrect Authorizatio n	25-09-2019	5	runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious			N/A		A-LIN-RUNC- 141019/212		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descrip	tion & CVE	ID	Pat	ch	NCII	PC ID
			Docker imag over a /proc CVE ID : CV	director	у.				
Linux-nfs									
nfs-utils									
Improper Privilege Management	19-09-2019	10	The nfs-utils package in SUSE Linux Enterprise Server 12 before and including version 1.3.0- 34.18.1 and in SUSE Linux Enterprise Server 15 before and including version 2.1.1- 6.10.2 the directory /var/lib/nfs is owned by statd:nogroup. This directory contains files owned and managed by root. If statd is compromised, it can therefore trick processes running with root privileges into creating/overwriting files anywhere on the system if fs.protected_symlinks is not set CVE ID : CVE-2019-3689		https:/ zilla.su m/sho g.cgi?id 50733	ise.co w_bu d=11	A-LIN-1 141019		
Logmein									
lastpass									
Insufficiently Protected Credentials	16-09-2019	5.8	LogMeIn Lat 4.33.0 allow construct a c that capture for a victim' previously v because do_ can be bypa clickjacking CVE ID : CV	N/A		A-LOG-LAST- 141019/214			
makandra									
CV Scoring Scale		1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
consul					
Incorrect Authorizatio n	23-09-2019	7.5	The makandra consul gem through 1.0.2 for Ruby has Incorrect Access Control. CVE ID : CVE-2019-16377	N/A	A-MAK-CONS- 141019/215
Mediawiki	I			I	
mediawiki					
Information Exposure	25-09-2019	5	In MediaWiki through 1.33.0, Special:Redirect allows information disclosure of suppressed usernames via a User ID Lookup.	N/A	A-MED-MEDI- 141019/216
			CVE ID : CVE-2019-16738		
Microfocus					
service_mana	ger			I	
Incorrect Authorizatio n	18-09-2019	6.5	Allow changes to some table by non-SysAdmin in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. This vulnerability could be exploited to allow unauthorized access and modification of data. CVE ID : CVE-2019-11661	https://soft waresuppor t.softwaregr p.com/doc/ KM035183 16	A-MIC-SERV- 141019/217
Information Exposure Through an Error Message	18-09-2019	4	Class and method names in error message in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. This vulnerability could be exploited in some special cases to allow information exposure through an error message.	https://soft waresuppor t.softwaregr p.com/doc/ KM035183 16	A-MIC-SERV- 141019/218

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				66						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2019-11662			
Insufficiently Protected Credentials	18-09-2019	4	Clear text credentials are used to access managers app in Tomcat in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow sensitive data exposure. CVE ID : CVE-2019-11663	https://soft waresuppor t.softwaregr p.com/doc/ KM035183 16	A-MIC-SERV- 141019/219	
Insufficiently Protected Credentials	18-09-2019	4	Clear text password in browser in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow sensitive data exposure. CVE ID : CVE-2019-11664	https://soft waresuppor t.softwaregr p.com/doc/ KM035183 16	A-MIC-SERV- 141019/220	
Information Exposure	17-09-2019	5	Data exposure in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow sensitive data exposure. CVE ID : CVE-2019-11665	https://soft waresuppor t.softwaregr p.com/doc/ KM035183 16	A-MIC-SERV- 141019/221	
Deserializati on of Untrusted Data	17-09-2019	6.8	Insecure deserialization of untrusted data in Micro Focus Service Manager product versions 9.30, 9.31, 9.32, 9.33, 9.34, 9.35, 9.40, 9.41, 9.50, 9.51, 9.52, 9.60, 9.61, 9.62. The vulnerability could be exploited to allow	ted data in Microhttps://softService Managerwaresupporct versions 9.30, 9.31,t.softwaregr.33, 9.34, 9.35, 9.40,p.com/doc/.50, 9.51, 9.52, 9.60,KM035183.62. The vulnerability16		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
				ure dese sted dat		on of				
				D : CVE -		1666				
Information Exposure	17-09-2019	5	Unaut conta Focus versic 9.52, vulne explo unaut privat	thorized ct inforn Service ons 9.41, 9.60, 9.6 rability ited to a chorized te data. D : CVE-	access t nation in Manage , 9.50, 9. 1, 9.62. could be llow access t	to n Micro er, 51, The e	https:, wares t.softw p.com KM03 46	uppor varegr /doc/	A-MIC-S 141019	
Microsoft			<u> </u>				<u> </u>			
forefront_end	lpoint_protect	tion_20	010							
Improper Input Validation	23-09-2019	5	vulne Micro impro 'Micro of Ser	ial of sen rability o soft Def operly ha osoft Def vice Vul D : CVE-	exists w ender andles fi fender D nerabili	les, aka)enial ty'.	N/A		A-MIC-FORE- 141019/224	
security_esse	ntials		<u>.</u>							
Improper Input Validation	23-09-2019	5	vulne Micro impro 'Micro of Ser	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'. CVE ID : CVE-2019-1255					A-MIC-S 141019	
system_cente	r_endpoint_p	rotecti	on							
Improper Input Validation	23-09-2019	5	vulne Micro impro 'Micro	ial of sen rability o soft Def operly ha osoft Def vice Vul	exists w ender andles fi fender D	les, aka)enial	N/A		A-MIC-SYST- 141019/226	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	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-2019-1255								
system_center_endpoint_protection_2012											
Improper Input Validation	23-09-2019	5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'. CVE ID : CVE-2019-1255	N/A	A-MIC-SYST- 141019/227						
windows_def	ender			L							
Improper Input Validation	23-09-2019	5	A denial of service vulnerability exists when Microsoft Defender improperly handles files, aka 'Microsoft Defender Denial of Service Vulnerability'.	N/A	A-MIC-WIND- 141019/228						
CVE ID : CVE-2019-1255											
internet_expl	orer										
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-09-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-1221. CVE ID : CVE-2019-1367	N/A	A-MIC-INTE- 141019/229						
moddable											
moddable											
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-09-2019	7.5	In XS 9.0.0 in Moddable SDK OS180329, there is a heap- based buffer overflow in fxBeginHost in xsAPI.c when called from fxRunDefine in xsRun.c, as demonstrated by crafted JavaScript code to	N/A	A-MOD- MODD- 141019/230						
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10						

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIPC ID			
			xst. CVE ID : CVE-2019-16366						
XS									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	16-09-2019	7.5	In XS 9.0.0 in Moddable SDK OS180329, there is a heap- based buffer overflow in fxBeginHost in xsAPI.c when called from fxRunDefine in xsRun.c, as demonstrated by crafted JavaScript code to xst. CVE ID : CVE-2019-16366	N/A		A-MOD-XS- 141019/231			
mz-automatio	on								
libiec61850									
Use After Free	19-09-2019	5	libIEC61850 through 1.3.3 has a use-after-free in MmsServer_waitReady in mms/iso_mms/server/mms _server.c, as demonstrated by server_example_goose. CVE ID : CVE-2019-16510	5 N/A		A-MZLIBI- 141019/232			
Netapp	I								
ontap_select_	deploy_admir	istrati	on_utility						
Improper Input Validation	24-09-2019	7.5	ONTAP Select Deploy administration utility versions 2.12 & 2.12.1 ship with an HTTP service bound to the network allowing unauthenticated remote attackers to perform administrative actions. CVE ID : CVE-2019-5504	N/A	A-NET-ON7 141019/23				
Insufficiently Protected Credentials	24-09-2019	5	ONTAP Select Deploy administration utility versions 2.2 through 2.12.1 transmit credentials in plaintext.	N/A		A-NET-ONTA- 141019/234			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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-2019-5505						
Netgate									
Pfsense									
Cross-Site Request Forgery (CSRF)	26-09-2019	9 6.8 diag_command.php in pfSense 2.4.4-p3 allows CSRF via the txtCommand o txtRecallBuffer field, as demonstrated by executing OS commands. This occurs because csrf_callback() produces a "CSRF token expired" error and a Try Again button when a CSRF token is missing.		N/A	A-NET-PFSE- 141019/235				
			CVE ID : CVE-2019-16667		_				
ImproperNeutralization of SpecialElementsused in an OSCommand('OSCommand		9	pfSense through 2.3.4 through 2.4.4-p3 allows Remote Code Injection via a methodCall XML document with a pfsense.exec_php call containing shell metacharacters in a parameter value.	N/A	A-NET-PFSE- 141019/236				
Injection')			CVE ID : CVE-2019-16701						
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	26-09-2019	4.3	An XSS issue was discovered in pfSense through 2.4.4-p3. In services_captiveportal_mac.p hp, the username and delmac parameters are displayed without sanitization.	N/A	A-NET-PFSE- 141019/237				
			CVE ID : CVE-2019-16914						
Improper Input Validation	26-09-2019	7.5	An issue was discovered in pfSense through 2.4.4-p3. widgets/widgets/picture.wi dget.php uses the widgetkey parameter directly without	N/A	A-NET-PFSE- 141019/238				

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				71						

Improper Neutralization and no S gath and the service size of input (Classic Developering Size of input (Classic Developering26-09-2019 size of no size of no<	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Netskope netskope netskope netskope netskope netskope netskope Buffer Copy without connections from localhost. https://sup port.netsko Classic Buffer 26-09-2019 7.2 suffers from a stack based https://sup A-NET-NETS- Buffer Overflow 'n 26-09-2019 7.2 The Netskope client service, us/articles/ usffers from a stack based buffer overflow in "doHandshakefromServer" function. Local users can use this vulnerability to trigger a crash of the service and potentially cause additional impact on the system. Netskope- Client A-NET-NETS- Improper Neutralizatio n of Special 26-09-2019 7.2 The Netskope client service, v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connections from localhost. The connection handling function in this service suffers from command injection vulnerability. Local users can use this vulnerability to execute code with NT\SYSTEM privilege. A-NET-NETS- 141019/240 7.2 7.2 The connection handling function in this service cols with NT\SYSTEM privilege. A-NET-NETS- 141019/240 7.2 7.2 7.2				basename call) for a pathname to file_get_contents or					
netskopeBuffer Copy without (Classic Buffer Overflow')26-09-20197.2The Netskope client service, v57 before 57.2.0.219 and v60 before 60.2.0.214, 				CVE ID : CVE-2019-16915					
Buffer Copy without Checking Size of Input ('Classic Buffer' Overflow')26-09-2019 26-09-20197.2The Netskope client service, v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM he connection handling function in this service suffers from a stack based buffer overflow in "doHandshakefromServer" function. Local users can use this vulnerability to trigger a crash of the service and potentially cause additional impact on the system. CVE D: CVE-2019-10882https://sup potentially cause additional impact on the system.https://sup potentially cause additional impact on the system.https://sup potentially cause additional impact on the system.https://sup potentially cause additional inpact on the system.https://sup potentially cause additional impact on the system.https://sup potentially cause additional impact on the system.https://sup potentially cause additional impact on the system.https://sup potentesties/ Stofer 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connections from locahost. The connection handling function in this service suffers from command injection vulnerability. Local users can use this vulnerability to execute code with NT\SYSTEM privilege. CVE ID: CVE-2019-12091https://sup advide A-NET-NETS- 141019/240CV scoring Scaleadd122d3d4d455667788990	netskope								
Buffer Copy without Checking Size of Input (Classic Buffer Overflow')26-09-20197.27.2Suffers from a stack based buffer overflow in "doHandshakefromServer" function in this service suffers from a stack based buffer overflow in "doHandshakefromServer" function. Local users can use this vulnerability to trigger a crash of the service and potentially cause additional impact on the system.Https://sup pot.netsko pe.com/hc/ en- us/articles/ 360014589 894- Netskope- ClientA-NET-NETS- 141019/239Improper Neutralizatio n of Special Elements used in an OS Command (I)26-09-20197.2The Netskope client service, v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connection handling function in this service suffers from command injection in this service suffers from command injection vulnerability. Local users can use this vulnerability to execute code with NT\SYSTEM privilege.A-NET-NETS- 141019/240Improper Neutralizatio n of Special Elements used in an OS (OS Command Injection')7.2The Netskope client service, v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connection handling function in this service suffers from command injection vulnerability. Local users can use this vulnerability to execute code with NT\SYSTEM privilege.A-NET-NETS- 141019/240VStoring Scale0.11.42.44.55.66.77.88.48.4	netskope								
Improper Neutralizatio n of Special Elements used in an OS (OS Command [105]CV Scoring Scale26-09-20197.2v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connections from localhost. The connection handling function in this service suffers from command injection vulnerability. Local users can use this vulnerability to execute code with NT\SYSTEM privilege.https://sup port.netsko pe.com/hc/ en- us/articles/ 360014589 894- Netskope- ClientA-NET-NETS- 141019/240CV Scoring Scale0.11.22.33.44.55.66.77.88.99.10	without Checking Size of Input ('Classic Buffer	26-09-2019	7.2	v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connections from localhost. The connection handling function in this service suffers from a stack based buffer overflow in "doHandshakefromServer" function. Local users can use this vulnerability to trigger a crash of the service and potentially cause additional impact on the system.	port.netsko pe.com/hc/ en- us/articles/ 360014589 894- Netskope-	_			
	Neutralizatio n of Special Elements used in an OS Command ('OS Command	26-09-2019	7.2	v57 before 57.2.0.219 and v60 before 60.2.0.214, running with NT\SYSTEM privilege, accepts network connections from localhost. The connection handling function in this service suffers from command injection vulnerability. Local users can use this vulnerability to execute code with NT\SYSTEM privilege.	port.netsko pe.com/hc/ en- us/articles/ 360014589 894- Netskope-				
	-	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
netty	I	<u> </u>			•		
netty							
Inconsistent Interpretatio n of HTTP Requests ('HTTP Request Smuggling')	26-09-2019	5	Netty before 4.1.42.Final mishandles whitespace before the colon in HTTP headers (such as a "Transfer-Encoding : chunked" line), which leads to HTTP request smuggling. CVE ID : CVE-2019-16869	N/A	A-NET-NETT- 141019/241		
ngiflib_projec	ct						
ngiflib							
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-09-2019	6.8	ngiflib 0.4 has a heap-based buffer overflow in WritePixel() in ngiflib.c when called from DecodeGifImg, because deinterlacing for small pictures is mishandled. CVE ID : CVE-2019-16346	N/A	A-NGI-NGIF- 141019/242		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-09-2019	6.8	ngiflib 0.4 has a heap-based buffer overflow in WritePixels() in ngiflib.c when called from DecodeGifImg, because deinterlacing for small pictures is mishandled. CVE ID : CVE-2019-16347	N/A	A-NGI-NGIF- 141019/243		
Open-emr	1			1			
openemr							
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site	16-09-2019	4.3	OpenEMR v5.0.1-6 allows XSS. CVE ID : CVE-2019-8368	N/A	A-OPE-OPEN- 141019/244		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Scripting')ImageImageImageImproper Control of Generation of Code ('Code Injection')16-09-201990OpenEMR v5.0.1-6 allows code execution. CVE ID : CVE-2019-8371N/AA-OPE-OPEI 141019/24.pac4jCVE ID : CVE-2019-8371N/AA-OPE-OPEI 141019/24.pac4jThe SAML identifier generated within SAML2Utils java was found to make use of the apache commons-lang3 RandomStringUtils class which makes them predictable due to RandomStringUtils class which makes them predictable due to RRN's algorithm not being cryptographically strong. This issue only affects the 3.X release of pac4j-saml. CVE ID : CVE-2019-10755N/AA-PAC-PACA 141019/24.pagekitThe Reset Password feature in Pagekit 1.0.17 gives a different response depending on whether the e- mail address of a valid user account is entered, which might make it easier for attackers to enumerate accounts. CVE ID : CVE-2019-16669N/AA-PAC-PACF A-PAC-PACFpam-python_projectUCVE ID : CVE-2019-16669N/AA-PAG-PAGF 141019/24.	Weakness	Publish Date	CVSS		Descripti	on & CVE	ID	Pat	ch	NCIIF	PC ID
Control of Generation of Code (Code (Injection))16-09-2019SOpenEMR v5.0.1-6 allows code execution. CVE ID : CVE-2019-8371N/AA-OPE-OPEI 141019/24 pac4j The SAML identifier generated within SAML2Utils java was found to make use of the apache commons-lang3 RandomStringUtils Class which makes them predictable due to Random StringUtils PRNG's algorithm not being cryptographically strong. This issue only affects the 3.X release of pac4j-samI.N/AA-PAC-PAC4 141019/24 pagekit The Reset Password feature might make it easier for ating algorithm not being cryptographically strong. This issue only affects the 3.X release of pac4j-samI.N/AA-PAC-PAC4 141019/24 Pagekitpagekit CUFE ID : CVE-2019-10755N/AA-PAG-PAGI 141019/24Information Exposure Through21-09-2019SThe Reset Password feature aligorithm not being cryptographically strong. This issue only affects the aligorithm colspanse different response depending on whether the e- mail address of a valid user account is entered, which might make it easier for attackers to enumerate accounts. CVE ID : CVE-2019-16669N/AA-PAG-PAGI 141019/24 Disc	Scripting')										
pac4jUse of Cryptographi cally Weak Pseudo- Random23-09-20194A-PAC-PACA predictable due to RandomStringUtils class which makes them predictable due to RandomStringUtils PRNG's algorithm not being cryptographically strong. This issue only affects the 3.X release of pac4j-saml. CVE ID : CVE-2019-10755N/AA-PAC-PACA A-PAC-PACA 141019/24 A-PAC-PACA 141019/24 A-PAC-PACA 141019/24 A-PAC-PACA A-PAC-PACA A-PAC-PACA A-PAC-PACA 141019/24 Mine due to predictable due to RandomStringUtils PRNG's algorithm not being cryptographically strong. This issue only affects the 3.X release of pac4j-saml. CVE ID : CVE-2019-10755N/AA-PAC-PACA A-P	Control of Generation of Code ('Code	16-09-2019	9	code	executio	n.		N/A			
Use of Cryptographi cally Weak Pseudo- Random23-09-20194The SAML identifier generated within SAML2Utilsjava was found to make use of the apache commons-lang3 RandomStringUtils class 	pac4j										
Use of Cryptographi cally Weak Pseudo- Random Number Generator (PRNG)23-09-20194generated within SAML2Utilsjava was found to make use of the apache commons-lang3 RandomStringUtils class which makes them predictable due to o RandomStringUtils PRNG's algorithm not being cryptographically strong. This issue only affects the 3.X release of pac4j-saml.N/AA-PAC-PAC4 A-PAC-PAC4 141019/240pagekit	pac4j										
pagekit Information Exposure Through Discrepancy Information Exposure Through Discrepancy Exposure Through Discrepancy Through Through Discrepancy Through Through Discrepancy Through Discrepancy Through	Cryptographi cally Weak Pseudo- Random Number Generator	23-09-2019	4	gener SAMI to ma comr Rand which predi Rand algor crypt This 3.X re	rated wit L2Utils.ja ake use o nons-lan omStrin h makes ictable d omStrin rithm not cographic issue on elease of	thin ava was of the ap g3 gUtils cl them ue to gUtils Pl being cally stru- y affects pac4j-sa	ache ass RNG's ong. s the aml.	N/A		_	-
Information Exposure Through Discrepancy21-09-20195The Reset Password feature in Pagekit 1.0.17 gives a different response depending on whether the e- mail address of a valid user account is entered, which might make it easier for attackers to enumerate accounts.N/AA-PAG-PAG A141019/24Pam-python_project	pagekit									<u> </u>	
Information Exposure Through Discrepancy21-09-20195in Pagekit 1.0.17 gives a different response depending on whether the e- mail address of a valid user account is entered, which might make it easier for attackers to enumerate accounts.N/AA-PAG-PAGI 141019/24Discrepancy EVENDEVENDDiscrepancy CVE ID : CVE-2019-16669Pam-python_project	pagekit										
	Exposure Through	21-09-2019	5	in Pa differ depe mail accou migh attac accou	in Pagekit 1.0.17 gives a different response depending on whether the e- mail address of a valid user account is entered, which might make it easier for attackers to enumerate accounts.						
pam-python	pam-python_	project								l	
	pam-python										
CV Scoring Scale	CV Scoring Scol	0									

(CVSS)				= 1						
CV Scoring Scale	0-1	1-2	2-3	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	24-09-2019	7.2	pam-python before 1.0.7-1 has an issue in regard to the default environment variable handling of Python, which could allow for local root escalation in certain PAM setups. CVE ID : CVE-2019-16729	N/A	A-PAM-PAM 141019/248
Phpbb					<u> </u>
phpbb					
Cross-Site Request Forgery (CSRF)	27-09-2019	4.3	phpBB version 3.2.7 allows the stealing of an Administration Control Panel session id by leveraging CSRF in the Remote Avatar feature. The CSRF Token Hijacking leads to stored XSS CVE ID : CVE-2019-13376	N/A	A-PHP-PHPB- 141019/249
Phpipam					1
phpipam					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom- fields/filter-result.php table parameter when action=add is used. CVE ID : CVE-2019-16692	N/A	A-PHP-PHPI- 141019/250
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom- fields/order.php table parameter when action=add is used. CVE ID : CVE-2019-16693	N/A	A-PHP-PHPI- 141019/251

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				75						

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	C ID		
Injection')												
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	inject app/a fields parar is use	PAM 1.4 ion via t admin/c /edit-re neter wh d. D : CVE -	he ustom- sult.php ien actio	table on=add	N/A		A-PHP-I 141019			
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	phpIPAM 1.4 allows SQL injection via the app/admin/custom- fields/filter.php table parameter when action=add is used. CVE ID : CVE-2019-16695			N/A		A-PHP-I 141019				
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	22-09-2019	7.5	inject app/a fields parar is use	phpIPAM 1.4 allows SQL injection via the app/admin/custom- fields/edit.php table parameter when action=add is used. CVE ID : CVE-2019-16696			N/A		A-PHP-I 141019			
phpmywind												
phpmywind												
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	23-09-2019	4.3	PHPM XSS.	admin/infolist_add.php in PHPMyWind 5.6 has stored XSS. CVE ID : CVE-2019-16703			PHPMyWind 5.6 has stored XSS.		N/A		A-PHP-I 141019	
Improper	23-09-2019	3.5	admi	admin/infoclass_update.php			N/A		A-PHP-I	PHPM-		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3				6-7	7-8	8-9	9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')			in PHPMyWind 5.6 has stored XSS. CVE ID : CVE-2019-16704		141019/256
pivotal_softwa					
pivotal_applic	cation_service	•		1	
Improper Privilege Management	20-09-2019	6.5	Pivotal Apps Manager, included in Pivotal Application Service versions 2.3.x prior to 2.3.18, 2.4.x prior to 2.4.14, 2.5.x prior to 2.5.10, and 2.6.x prior to 2.6.5, contains an invitations microservice which allows users to invite others to their organizations. A remote authenticated user can gain additional privileges by inviting themselves to spaces that they should not have access to. CVE ID : CVE-2019-11280	https://piv otal.io/secu rity/cve- 2019- 11280	A-PIV-PIVO- 141019/257
plutinosoft					1
platinum					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	26-09-2019	5	Platinum UPnP SDK 1.2.0 allows Directory Traversal in Core/PltHttpServer.cpp because it checks for / where it should be checking for/ instead. CVE ID : CVE-2019-16903	N/A	A-PLU-PLAT- 141019/258
portaudio-rs_	project			I	I
portaudio-rs					
Use After	25-09-2019	7.5	An issue was discovered in	https://rust	A-POR-PORT-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Free			the portaudio-rs crate through 0.3.1 for Rust. There is a use-after-free with resultant arbitrary code execution because of a lack of unwind safety in stream_callback and stream_finished_callback.	sec.org/adv isories/RUS TSEC-2019- 0022.html	141019/259	
			CVE ID : CVE-2019-16881			
prise						
adas						
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	An issue was discovered in PRiSE adAS 1.7.0. The OPENSSO module does not properly escape output on error, leading to reflected XSS. CVE ID : CVE-2019-14911	N/A	A-PRI-ADAS- 141019/260	
URL Redirection to Untrusted Site ('Open Redirect')	20-09-2019	5.8	An issue was discovered in PRiSE adAS 1.7.0. The OPENSSO module does not properly check the goto parameter, leading to an open redirect that leaks the session cookie. CVE ID : CVE-2019-14912	N/A	A-PRI-ADAS- 141019/261	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	3.5	An issue was discovered in PRiSE adAS 1.7.0. Log data are not properly escaped, leading to persistent XSS in the administration panel. CVE ID : CVE-2019-14913	N/A	A-PRI-ADAS- 141019/262	
Improper Limitation of a Pathname to a	20-09-2019	7.5	An issue was discovered in PRiSE adAS 1.7.0. The path is not properly escaped in the medatadata_del method,	N/A	A-PRI-ADAS- 141019/263	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			leading to an arbitrary file read and deletion via Directory Traversal. CVE ID : CVE-2019-14914		
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	An issue was discovered in PRiSE adAS 1.7.0. Certificate data are not properly escaped. This leads to XSS when submitting a rogue certificate. CVE ID : CVE-2019-14915	N/A	A-PRI-ADAS- 141019/264
Unrestricted Upload of File with Dangerous Type	20-09-2019	4	An issue was discovered in PRiSE adAS 1.7.0. A file's format is not properly checked, leading to an unrestricted file upload. CVE ID : CVE-2019-14916	N/A	A-PRI-ADAS- 141019/265
Insufficiently Protected Credentials	20-09-2019	5	An issue was discovered in PRiSE adAS 1.7.0. The current database password is embedded in the change password form. CVE ID : CVE-2019-15085	N/A	A-PRI-ADAS- 141019/266
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	An issue was discovered in PRiSE adAS 1.7.0. The newentityID parameter is not properly escaped, leading to a reflected XSS in the error message. CVE ID : CVE-2019-15086	N/A	A-PRI-ADAS- 141019/267
Missing Authorizatio n	20-09-2019	6.5	An issue was discovered in PRiSE adAS 1.7.0. An authenticated user can change the function used to hash passwords to any function, leading to remote	N/A	A-PRI-ADAS- 141019/268

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				70						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution.		
			CVE ID : CVE-2019-15087		
Incorrect Type Conversion or Cast	20-09-2019	7.5	An issue was discovered in PRiSE adAS 1.7.0. Password hashes are compared using the equality operator. Thus, under specific circumstances, it is possible to bypass login authentication. CVE ID : CVE-2019-15088	N/A	A-PRI-ADAS- 141019/269
Cross-Site Request Forgery (CSRF)	20-09-2019	6.8	An issue was discovered in PRiSE adAS 1.7.0. Forms have no CSRF protection, letting an attacker execute actions as the administrator. CVE ID : CVE-2019-15089	N/A	A-PRI-ADAS- 141019/270
publisure					
publisure					
Unrestricted Upload of File with Dangerous Type	18-09-2019	6.5	An issue was discovered in the secure portal in Publisure 2.1.2. Once successfully authenticated as an administrator, one is able to inject arbitrary PHP code by using the adminCons.php form. The code is then stored in the E:\PUBLISURE\webservice\ webpages\AdminDir\Templ ates\ folder even if removed from the adminCons.php view (i.e., the rogue PHP file can be hidden). CVE ID : CVE-2019-14252	N/A	A-PUB-PUBL- 141019/271
Incorrect Authorizatio n	18-09-2019	6.4	An issue was discovered in servletcontroller in the secure portal in Publisure	N/A	A-PUB-PUBL- 141019/272
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIF	PC ID
			authe a que the //	One can enticatio ry on PH AdminDi d be res	n and pe IP forms ir folder	erform Swithin				
			CVE I	D : CVE	2019-1	4253				
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	18-09-2019	7.5	An issue was discovered in the secure portal in Publisure 2.1.2. Because SQL queries are not well sanitized, there are multiple SQL injections in userAccFunctions.php functions. Using this, an attacker can access passwords and/or grant access to the user account "user" in order to become "Administrator" (for example). CVE ID : CVE-2019-14254				N/A		A-PUB- 141019	
Pydio	<u> </u>		<u> </u>				<u> </u>		<u> </u>	
pydio										
Information Exposure Through an Error Message	19-09-2019	5	Pydio 6.0.8 mishandles error reporting when a directory allows unauthenticated uploads, and the remote- upload option is used with the http://localhost:22 URL. The attacker can obtain sensitive information such as the name of the user who created that directory and other internal server information. CVE ID : CVE-2019-15032			N/A		A-PYD- 141019		
Server-Side Request Forgery	19-09-2019	4	Pydio 6.0.8 allows Authenticated SSRF during a Remote Link Feature				N/A		A-PYD- 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	Pat	tch	NCIIP	C ID	
(SSRF)			download. An attacker can specify an intranet address in the file parameter to index.php, when sending a file to a remote server, as demonstrated by the file=http%3A%2F%2F192.1 68.1.2 substring.							
			CVE I	D : CVE	2019-1	5033				
Qemu										
qemu										
Loop with Unreachable Exit Condition ('Infinite Loop')	24-09-2019	5	12+de 6+del 8~de 8+del 12+de execu lsi_ex scsi a advar read t lead t next o the ex 10k it cover well.	MU 1:4.7 eb8u6, 1 b9u8, 1:7 b10u1, 1 b10u2, a eb8u12 iting scri ecute_sc dapter e nces 's-> next opc dapter e nces 's-> next opc co an infi opcode if kisting lo terations rs no-op D : CVE -	:2.8+dfs 3.1+dfsg 1:3.1+dfs nd 1:2.1 (fixed), v ipt in rript(), tl mulator dsp' ind ode. Thi nite loop s empty oop exit s so that opcodes	eg- sg- sg- +dfsg- when ne LSI ex to s can p if the after it as	N/A		A-QEM- QEMU- 141019	
Radare radare2										
			In	laro? h-	for 20	0.0				
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command	23-09-2019	6.8	In radare2 before 3.9.0, a command injection vulnerability exists in bin_symbols() in libr/core/cbin.c. By using a crafted executable file, it's possible to execute arbitrary shell commands with the				N/A		A-RAD- 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			permissions of the victim. This vulnerability is due to an insufficient fix for CVE- 2019-14745 and improper handling of symbol names embedded in executables.		
			CVE ID : CVE-2019-16718		
redlion	<u> </u>				
crimson					
Use of Hard- coded Credentials	23-09-2019	4.3	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, uses a hard-coded password to encrypt protected files in transit and at rest, which may allow an attacker to access configuration files. CVE ID : CVE-2019-10990	N/A	A-RED-CRIM- 141019/278
Use After Free	23-09-2019	6.8	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that can reference memory after it has been freed. CVE ID : CVE-2019-10996	N/A	A-RED-CRIM- 141019/279
Improper Restriction of Operations within the Bounds of a Memory Buffer	23-09-2019	6.8	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that operates outside of the	N/A	A-RED-CRIM- 141019/280
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7·	-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patcl	h	NCIIPC	ID
			designated memory area.				
			CVE ID : CVE-2019-10978				
Access of Uninitialized Pointer	23-09-2019	6.8	Red Lion Controls Crimson, version 3.0 and prior and version 3.1 prior to release 3112.00, allow multiple vulnerabilities to be exploited when a valid user opens a specially crafted, malicious input file that causes the program to mishandle pointers. CVE ID : CVE-2019-10984	N/A	N/A		RIM- 281
redmineup							
crm							
Improper							
Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	16-09-2019	4.3	The CRM Plugin before 4.2.4 for Redmine allows XSS via crafted vCard data. CVE ID : CVE-2019-15950	N/A		A-RED-CF 141019/2	
reputeinfosys	stems						
arforms							
Improper Input Validation	27-09-2019	6.4	In the ARforms plugin 3.7.1 for WordPress, arf_delete_file in arformcontroller.php allows unauthenticated deletion of an arbitrary file by supplying the full pathname. CVE ID : CVE-2019-16902	N/A		A-REP-AR 141019/2	
riot-os							
riot							
NULL Pointer	24-09-2019	5	RIOT 2019.07 contains a NULL pointer dereference in	N/A		A-RIO-RIO 141019/2	
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)			84				

Weakness	Publish Date	CVSS		Descriptio	on & CVE	Pat	tch	NCIIP	C ID	
Dereference			<pre>implementation (asymcute), potentially allowing an attacker to crash a network node running RIOT. This requires spoofing an MQTT server response. To do so, the attacker needs to know the MQTT MsgID of a pending MQTT protocol message and the ephemeral port used by RIOT's MQTT implementation. Additionally, the server IP address is required for spoofing the packet. CVE ID : CVE-2019-16754</pre>							
Rockwellauto	mation			DICVE	-2019-1	0754				
arena_simula		•								
Access of Uninitialized Pointer	24-09-2019	6.8	In Rockwell Automation Arena Simulation Software Cat. 9502-Ax, Versions 16.00.00 and earlier, a maliciously crafted Arena file opened by an unsuspecting user may result in the use of a pointer that has not been initialized. CVE ID : CVE-2019-13527			N/A		A-ROC-4 141019		
RSA										
bsafe_cert-j			DQ:			_				
Improper Verification of Cryptographi c Signature	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Improper Verification of Cryptographic Signature vulnerability. A malicious remote attacker could potentially exploit this vulnerability to coerce two				N/A		A-RSA-F 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parties into computing the same predictable shared key		
			CVE ID : CVE-2019-3738		
Information Exposure Through Discrepancy	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to Information Exposure Through Timing Discrepancy vulnerabilities during ECDSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover ECDSA keys. CVE ID : CVE-2019-3739	7	A-RSA-BSAF- 141019/287
Information Exposure	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Information Exposure Through Timing Discrepancy vulnerabilities during DSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover DSA keys.		A-RSA-BSAF- 141019/288
			CVE ID : CVE-2019-3740		
bsafe_ssl-j	_	-			_
Improper Verification of Cryptographi c Signature	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Improper Verification of Cryptographic Signature vulnerability. A malicious remote attacker could potentially exploit this vulnerability to coerce two parties into computing the same predictable shared key CVE ID : CVE-2019-3738	N/A	A-RSA-BSAF- 141019/289
Information	18-09-2019	4.3	RSA BSAFE Crypto-J versions	; N/A	A-RSA-BSAF-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	۱	NCIIPC ID
Exposure Through Discrepancy			prior to 6.2.5 are vulnerable to Information Exposure Through Timing Discrepancy vulnerabilities during ECDSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover ECDSA keys. CVE ID : CVE-2019-3739			141019/290
Information Exposure	18-09-2019	4.3	RSA BSAFE Crypto-J versions prior to 6.2.5 are vulnerable to an Information Exposure Through Timing Discrepancy vulnerabilities during DSA key generation. A malicious remote attacker could potentially exploit those vulnerabilities to recover DSA keys. CVE ID : CVE-2019-3740	N/A		A-RSA-BSAF- 141019/291
archer			I			
Information Exposure	18-09-2019	4	RSA Archer, versions prior to 6.6 P3 (6.6.0.3), contain an information disclosure vulnerability. Information relating to the backend database gets disclosed to low-privileged RSA Archer users' UI under certain error conditions. CVE ID : CVE-2019-3756	N/A		A-RSA-ARCH- 141019/292
Improper Authenticati on	18-09-2019	7.5	RSA Archer, versions prior to 6.6 P2 (6.6.0.2), contain an improper authentication vulnerability. The vulnerability allows sysadmins to create user accounts with insufficient	N/A		A-RSA-ARCH- 141019/293
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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. Unauthenticated attackers could gain unauthorized access to the system using those accounts.				
			CVE ID : CVE-2019-3758				
sahipro							
sahi_pro	I			I			
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-09-2019	5	Within Sahi Pro 8.0.0, an attacker can send a specially crafted URL to include any victim files on the system via the script parameter on the Script_view page. This will result in file disclosure (i.e., being able to pull any file from the remote victim application). This can be used to steal and obtain sensitive config and other files. This can result in complete compromise of the application. The script parameter is vulnerable to directory traversal and both local and remote file inclusion. CVE ID : CVE-2019-13063	N/A		A-SAH-SAHI 141019/294	
Schneider-ele	ectric						
somachine_hv	vac						
Untrusted Search Path	17-09-2019	6.8	A CWE-426: Untrusted Search Path vulnerability exists in SoMachine HVAC v2.4.1 and earlier versions, which could cause arbitrary code execution on the system running SoMachine HVAC when a malicious DLL library is loaded by the	https://w w.schneid electric.co /en/down ad/docum nt/SEVD- 2019-225 04/	ler om nlo ne	A-SCH-SOMA 141019/295	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-1	10

Weakness	Publish Date	CVSS	Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
			product.						
			CVE ID : CVE-	2019-68	826				
Silverstripe									
silverstripe									
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	26-09-2019	3.5	In SilverStripo 4.0, there is X managed thro CVE ID : CVE -	https://w.silve pe.org nload/ ity- releas E-201 14272	erstri /dow /secur es/CV 9-	A-SIL-S 141019			
Files or Directories Accessible to External Parties	26-09-2019	5	In SilverStripe there is broke control on file CVE ID : CVE -	en access es.		https:/ w.silve pe.org nload/ ity- releas E-201 14273	erstri /dow /secur es/CV 9-	A-SIL-S 141019	
Session Fixation	25-09-2019	3.7	SilverStripe th allows session "change passy CVE ID : CVE-	n fixation word" for	i in the rm.	https:, w.silve pe.org nload, ity- releas E-201 12203	erstri /dow /secur es/CV 9-	A-SIL-S 141019	
Improper Privilege Management	25-09-2019	7.5	In SilverStripe through 4.3.3, a missing warning about leaving install.php in a public webroot can lead to unauthenticated admin access. CVE ID : CVE-2019-12204		https:, w.silve pe.org nload, ity- releas E-201 12204	erstri /dow /secur es/CV 9-	A-SIL-S 141019		
Improper Neutralizatio n of Input	25-09-2019	4.3	SilverStripe through 4.3.3 has Flash Clipboard			https://ww w.silverstri pe.org/dow		A-SIL-S 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Reflected XSS. CVE ID : CVE-2019-12205	nload/secur ity- releases/CV E-2019- 12205	
Information Exposure	25-09-2019	5	SilverStripe through 4.3.3 has incorrect access control for protected files uploaded via Upload::loadIntoFile(). An attacker may be able to guess a filename in silverstripe/assets via the AssetControlExtension. CVE ID : CVE-2019-12245	https://ww w.silverstri pe.org/dow nload/secur ity- releases/CV E-2019- 12245	A-SIL-SILV- 141019/301
Improper Privilege Management	26-09-2019	4	In SilverStripe through 4.3.3, there is access escalation for CMS users with limited access through permission cache pollution. CVE ID : CVE-2019-12617	https://ww w.silverstri pe.org/dow nload/secur ity- releases/CV E-2019- 12617	A-SIL-SILV- 141019/302
Spip	I				
spip					
Incorrect Authorizatio n	17-09-2019	4	SPIP before 3.1.11 and 3.2 before 3.2.5 allows authenticated visitors to modify any published content and execute other modifications in the database. This is related to ecrire/inc/meta.php and ecrire/inc/securiser_action. php. CVE ID : CVE-2019-16391	N/A	A-SPI-SPIP- 141019/303
Improper Neutralizatio n of Input During Web	17-09-2019	4.3	SPIP before 3.1.11 and 3.2 before 3.2.5 allows prive/formulaires/login.php	N/A	A-SPI-SPIP- 141019/304
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	l	Descriptio	on & CVE	ID	Pa	tch	NCIIP	PC ID
Page			XSS v	ia error	message	es.				
Generation ('Cross-site Scripting')			CVE I	D : CVE-	2019-1	6392				
URL Redirection to Untrusted Site ('Open Redirect')	17-09-2019	5.8	befor redire ecrire a %01 chara	before 3. e 3.2.5 m ect URLs e/inc/he D, %0A, o cter. D : CVE -	nishandl in aders.pl or %20	les hp with	N/A	N/A		PIP- 9/305
Information Exposure	17-09-2019	5	beford differ from page an e-r which to end	before 3. e 3.2.5 p ent erro the pass dependi nail add n might h umerate D : CVE -	rovides r messa word-re ng on wi ress exis nelp atta subscril	ges eminder hether sts, ickers bers.	N/A		A-SPI-S 141019	
	• •		CVEI	D:CVE-	2019-1	6394				
string-interne										
string-interne	er						1			
Use After Free	25-09-2019	5	the st befor allow from assoc point clonin	sue was o ring-into e 0.7.1 fo s attacko memory iated wi ers, beca ng flaw. D : CVE-	erner cra or Rust. ers to re location th dangl nuse of a	ate It ad ns ling	https: sec.or isories TSEC- 0023.l	g/adv g/RUS 2019-	A-STR-5 141019	
suricata-ids			UT LI	DICIE	_017 1					
suricata										
Out-of- bounds Read	24-09-2019	6.4	app-la 4.1.4. corru	An issue was discovered in app-layer-ssl.c in Suricata4.1.4. Upon receiving a corrupted SSLv3 (TLS 1.2) packet, the parser function		N/A		A-SUR-5 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID		
			TLSDecodeHSHelloExtensio ns tries to access a memory region that is not allocated, because the expected length of HSHelloExtensions does not match the real length of the HSHelloExtensions part of the packet. CVE ID : CVE-2019-15699						
Out-of- bounds Read	24-09-2019	6.4	An issue was discovered in Suricata 4.1.4. By sending multiple fragmented IPv4 packets, the function Defrag4Reassemble in defrag.c tries to access a memory region that is not allocated, because of a lack of header_len checking. CVE ID : CVE-2019-16410	N/A		A-SUR-S 141019			
Out-of- bounds Read	24-09-2019	7.5	An issue was discovered in Suricata 4.1.4. By sending multiple IPv4 packets that have invalid IPv4Options, the function IPV4OptValidateTimestamp in decode-ipv4.c tries to access a memory region that is not allocated. There is a check for o->len < 5 (corresponding to 2 bytes of header and 3 bytes of data). Then, "flag = *(o->data + 3)" places one beyond the 3 bytes, because the code should have been "flag = *(o- >data + 1)" instead. CVE ID : CVE-2019-16411	N/A		A-SUR-S 141019			
Symantec									
norton_passw		•							
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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	17-09-2019	2.1	Norton Password Manager, prior to 6.5.0.2104, may be susceptible to an information disclosure issue, which is a type of vulnerability whereby there is an unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information. CVE ID : CVE-2019-12755	https://sup port.symant ec.com/us/ en/article.S YMSA1493. html	A-SYM-NORT- 141019/311
Teampass					
teampass					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	26-09-2019	3.5	TeamPass 2.1.27.36 allows Stored XSS by setting a crafted password for an item in a common available folder or sharing the item with an admin. (The crafted password is exploitable when viewing the change history of the item or tapping on the item.) CVE ID : CVE-2019-16904	N/A	A-TEA-TEAM- 141019/312
terrasoft					
bpm_online_c		lk			
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	18-09-2019	7.5	A SQL injection vulnerability in the method Terrasoft.Core.DB.Column.C onst() in Terrasoft Bpm'online CRM-System SDK 7.13 allows attackers to execute arbitrary SQL commands via the value parameter. CVE ID : CVE-2019-15301	N/A	A-TER-BPM 141019/313
thinksaas					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinksaas					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	3.5	An issue was discovered in ThinkSAAS 2.91. There is XSS via the index.php?app=group∾=cr eate&ts=do groupname parameter. CVE ID : CVE-2019-16664	N/A	A-THI-THIN- 141019/314
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	4.3	An issue was discovered in ThinkSAAS 2.91. There is XSS via the content to the index.php?app=group∾=c omment&ts=do&js=1 URI, as demonstrated by a crafted SVG document in the SRC attribute of an EMBED element. CVE ID : CVE-2019-16665	N/A	A-THI-THIN- 141019/315
Tibco					
enterprise_ru	intime_for_r				
Improper Input Validation	https://ww w.tibco.com /support/a dvisories/2 019/09/tib co-security- advisory- september- 17-2019- tibco- enterprise- runtime- for-r- server- 2019- 11210	A-TIB-ENTE- 141019/316			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Analytics Platform for AWS Marketplace versions 10.4.0 and 10.5.0. CVE ID : CVE-2019-11210		
Improper Input Validation	18-09-2019	9	The server component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, and TIBCO Spotfire Analytics Platform for AWS Marketplace contains a vulnerability that theoretically allows an authenticated user to trigge remote code execution in certain circumstances. When the affected component run with the containerized TERI service on Linux the host ca theoretically be tricked into running malicious code. Thi issue affects: TIBCO Enterprise Runtime for R - Server Edition version 1.2.0 and below, and TIBCO Spotfire Analytics Platform for AWS Marketplace 10.4.0 10.5.0. CVE ID : CVE-2019-11211	https://ww w.tibco.com /support/a dvisories/2 r 019/09/tib co-security- advisory- september- 17-2019- tibco- enterprise- for-r- server- 2019- 11211	A-TIB-ENTE- 141019/317
spotfire_analy	tica platform	for a			
Improper Input Validation	18-09-2019	10	The server component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, and TIBCO Spotfire Analytics Platform for AWS Marketplace contains a vulnerability that theoretically allows an unauthenticated user to bypass access controls and remotely execute code using	/support/a dvisories/2 019/09/tib co-security- advisory- september- 17-2019- tibco-	A-TIB-SPOT- 141019/318
CV Scoring Scale				6-7 7-8	

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
			the operating system account hosting the affected component. This issue affects: TIBCO Enterprise Runtime for R - Server Edition versions 1.2.0 and below, and TIBCO Spotfire Analytics Platform for AWS Marketplace versions 10.4.0 and 10.5.0.				runtin for-r- server 2019- 11210	-		
Improper Input Validation	18-09-2019	9	CVE ID : CVE-2019-11210 The server component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, and TIBCO Spotfire Analytics Platform for AWS Marketplace contains a vulnerability that theoretically allows an authenticated user to trigger remote code execution in certain circumstances. When the affected component runs with the containerized TERR service on Linux the host can theoretically be tricked into running malicious code. This issue affects: TIBCO Enterprise Runtime for R - Server Edition version 1.2.0 and below, and TIBCO Spotfire Analytics Platform for AWS Marketplace 10.4.0; 10.5.0. CVE ID : CVE-2019-11211				https:, w.tibc /supp dvisor 019/0 co-sec adviso septer 17-20 tibco- enterp runtin for-r- server 2019- 11211	o.com ort/a ies/2 9/tib urity- ory- nber- 19- orise- ne-	A-TIB-S 141019	
totaldefense			•							
anti-virus										
Improper Privilege	24-09-2019	4.6	In Total Defense Anti-virus 9.0.0.773, insecure access			N/A		A-TOT- 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pate	ch	NCIII	PC ID
Management			%PRC efense used l allow hijack which escala ccSch the ex	control for the directory %PROGRAMDATA%\TotalD efense\Consumer\ISS\9\ used by ccschedulersvc.exe allows local attackers to hijack dotnetproxy.exe, which leads to privilege escalation when the ccSchedulerSVC service runs the executable. CVE ID : CVE-2019-13355						
Improper Privilege Management	24-09-2019	4.6	In Total Defense Anti-virus 9.0.0.773, insecure access control for the directory %PROGRAMDATA%\TotalD efense\Consumer\ISS\9\bd \TDUpdate2\ used by AMRT.exe allows local attackers to hijack bdcore.dll, which leads to privilege escalation when the AMRT service loads the DLL. CVE ID : CVE-2019-13356				N/A		A-TOT- 141019	
Untrusted Search Path	24-09-2019	4.6	In Total Defense Anti-virus 9.0.0.773, resource acquisition from the untrusted search path C:\ used by caschelp.exe allows local attackers to hijack ccGUIFrm.dll, which leads to code execution. SYSTEM- level code execution can be achieved when the ccSchedulerSVC service runs the affected executable. CVE ID : CVE-2019-13357				N/A		A-TOT- 141019	
traveloka traveloka										
CV Scoring Scal										
(CV Scoring Scar	0-1	1-2	2-3	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 Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	2.6	The Traveloka application 3.14.0 for Android exports com.traveloka.android.activi ty.common.WebViewActivity , leading to the opening of arbitrary URLs, which can inject deceptive content into the UI. (When in physical possession of the device, opening local files is also possible.) NOTE: As of 2019- 09-23, the vendor has not agreed that this issue has serious impact. The vendor states that the issue is not critical because it does not allow Elevation of Privilege, Sensitive Data Leakage, or any critical unauthorized activity from a malicious user. The vendor also states that a victim must first install a malicious APK to their application. CVE ID : CVE-2019-16681	N/A	A-TRA-TRAV- 141019/323
trusteddomai	in				
opendmarc					
Authenticati on Bypass by Spoofing	17-09-2019	7.5	OpenDMARC through 1.3.2 and 1.4.x through 1.4.0- Beta1 is prone to a signature-bypass vulnerability with multiple From: addresses, which might affect applications that consider a domain name to be relevant to the origin of an e-mail message. CVE ID : CVE-2019-16378	N/A	A-TRU-OPEN- 141019/324
tuzicms	l			L	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 98	6-7 7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tuzicms					
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-09-2019	7.5	App\Home\Controller\Zhua ntiController.class.php in TuziCMS 2.0.6 has SQL injection via the index.php/Zhuanti/group?id = substring. CVE ID : CVE-2019-16644	N/A	A-TUZ-TUZI- 141019/325
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	21-09-2019	4.3	TuziCMS 2.0.6 has XSS via the PATH_INFO to a group URI, as demonstrated by index.php/article/group/id/ 2/. CVE ID : CVE-2019-16657	N/A	A-TUZ-TUZI- 141019/326
Cross-Site Request Forgery (CSRF)	21-09-2019	6.8	TuziCMS 2.0.6 has index.php/manage/notice/d o_add CSRF. CVE ID : CVE-2019-16658	N/A	A-TUZ-TUZI- 141019/327
Cross-Site Request Forgery (CSRF)	21-09-2019	6.8	TuziCMS 2.0.6 has index.php/manage/link/do_ add CSRF. CVE ID : CVE-2019-16659	N/A	A-TUZ-TUZI- 141019/328
Upredsun					
file_sharing_v	vizard				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	7.5	File Sharing Wizard 1.5.0 allows a remote attacker to obtain arbitrary code execution by exploiting a Structured Exception Handler (SEH) based buffer overflow in an HTTP POST parameter, a similar issue to CVE-2010-2330 and CVE- 2010-2331.	N/A	A-UPR-FILE- 141019/329
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	l	Descriptio	on & CVE	ID	Pa	tch	NCIIP	CID
			CVE I	D : CVE-	2019-1	6724				
Valvesoftwar	e		<u> </u>							
counter-strik	e:_global_offe	nsive								
Improper Input Validation	19-09-2019	6.8	vphysics.dll in Counter- Strike: Global Offensive before 1.37.1.1 allows remote attackers to achieve code execution or denial of service by creating a gaming server and inviting a victim to this server, because a crafted map is mishandled during a memset call. CVE ID : CVE-2019-15943				https:, ub.cor s/CVE /mast E-201 15943 DME.r	n/bi7 /blob er/CV 9- 8/REA	A-VAL-(141019	
Vbulletin			<u> </u>							
vbulletin										
Improper Input Validation	24-09-2019	7.5	allow execu widge paran ajax/n route	vBulletin 5.x through 5.5.4 allows remote command execution via the widgetConfig[code] parameter in an ajax/render/widget_php routestring request. CVE ID : CVE-2019-16759					A-VBU- 141019	
Vmware			1							
workstation										
Out-of- bounds Read	20-09-2019	5.5	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650- 201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6) and Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain an out-of-bounds read vulnerability in the pixel shader functionality. Successful exploitation of				https:/ w.vmv om/se y/adv s/VMS 2019- 0012.J	ware.c ecurit isorie SA-	A-VMW WORK- 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Dat	e CVSS		Descripti	on & CVE	ID	Pat	tch	NCIIP	C ID
			infor may a norm creat cond Explo requi acces with is not ESXi defau Fusio	this issue may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on the host. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion. CVE ID : CVE-2019-5521						
fusion							<u> </u>			
Out-of- bounds Read	20-09-201	9 5.5	ESXie 6.5 b 2019 (15.x befor (11.x befor out-o vulne shade Succe this i infor may a norm creat cond Explo requi acces with	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650- 201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6) and Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain an out-of-bounds read vulnerability in the pixel shader functionality. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on the host. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on		https:, w.vmv om/se y/adv s/VMS 2019- 0012.J	vare.c curit isorie GA-	A-VMW 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				101						

			default on Workstation and Fusion. CVE ID : CVE-2019-5521							
L			CVE I	D : CVE	2019-5	521				
vcenter_server										
Insufficient Session 18-0 Expiration	09-2019	5.8	VMware vSphere ESXi (6.7 prior to ESXi670- 201810101-SG, 6.5 prior to ESXi650-201811102-SG, and 6.0 prior to ESXi600- 201807103-SG) and VMware vCenter Server (6.7 prior to 6.7 U1b, 6.5 prior to 6.5 U2b, and 6.0 prior to 6.0 U3j) contain an information disclosure vulnerability in clients arising from insufficient session expiration. An attacker with physical access or an ability to mimic a websocket connection to a user?s browser may be able to obtain control of a VM Console after the user has logged out or their session has timed out. CVE ID : CVE-2019-5531				http:// w.vmv om/se y/advi s/VMS 2019- 0013.l	vare.c ecurit isorie SA-	A-VMW VCEN- 141019	
Insufficiently Protected 18-0 Credentials	09-2019	4	VMware vCenter Server (6.7.x prior to 6.7 U3, 6.5 prior to 6.5 U3 and 6.0 prior to 6.0 U3j) contains an information disclosure vulnerability due to the logging of credentials in plain-text for virtual machines deployed through OVF. A malicious user with access to the log files containing vCenter OVF- properties of a virtual				https:, w.vmv om/se y/advi s/VMS 2019- 0013.l	vare.c ecurit isorie SA-	A-VMW VCEN- 141019	
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			machine deployed from an OVF may be able to view the credentials used to deploy the OVF (typically the root account of the virtual machine).		
			CVE ID : CVE-2019-5532 VMware vCenter Server		
Insufficiently Protected Credentials	18-09-2019	4	 VMware VCenter Server (6.7.x prior to 6.7 U3, 6.5 prior to 6.5 U3 and 6.0 prior to 6.0 U3j) contains an information disclosure vulnerability where Virtual Machines deployed from an OVF could expose login information via the virtual machine's vAppConfig properties. A malicious actor with access to query the vAppConfig properties of a virtual machine deployed from an OVF may be able to view the credentials used to deploy the OVF (typically the root account of the virtual machine). 	https://ww w.vmware.c om/securit y/advisorie s/VMSA- 2019- 0013.html	A-VMW- VCEN- 141019/336
vsphere_esxi	L				
Insufficient Session Expiration	18-09-2019	5.8	VMware vSphere ESXi (6.7 prior to ESXi670- 201810101-SG, 6.5 prior to ESXi650-201811102-SG, and 6.0 prior to ESXi600- 201807103-SG) and VMware vCenter Server (6.7 prior to 6.7 U1b, 6.5 prior to 6.5 U2b, and 6.0 prior to 6.0 U3j) contain an information disclosure vulnerability in clients arising from	om/securit	A-VMW- VSPH- 141019/337
				•	

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIPC ID
			insufficient session expiration. An attacker with physical access or an ability to mimic a websocket connection to a user?s browser may be able to obtain control of a VM Console after the user has logged out or their session has timed out.			
			CVE ID : CVE-2019-5531			
Webkul						
bagisto	Γ			T		1
Incorrect Authorizatio n	18-09-2019	6.5	In Webkul Bagisto before 0.1.5, the functionalities for customers to change their own values (such as address, review, orders, etc.) can also be manipulated by other customers. CVE ID : CVE-2019-16403	N/A		A-WEB-BAGI- 141019/338
Wolfssl						
wolfssl						
Out-of- bounds Read	24-09-2019	7.5	In wolfSSL through 4.1.0, there is a missing sanity check of memory accesses in parsing ASN.1 certificate data while handshaking. Specifically, there is a one- byte heap-based buffer over- read in CheckCertSignature_ex in wolfcrypt/src/asn.c. CVE ID : CVE-2019-16748	N/A		A-WOL- WOLF- 141019/339
wtcms_projec						
wtcms						
Cross-Site	23-09-2019	4.3	WTCMS 1.0 allows	N/A		A-WTC-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 104	6-7	7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	tch	NCIIP	C ID	
Request Forgery (CSRF)			index.php?g=admin&m=inde x&a=index CSRF with resultant XSS.					WTCM- 141019	/340	
			CVE ID : CVE-2019-16719							
yejiao										
tuzicms										
Improper Neutralizatio n of Special Elements used in an SQL Command ('SQL Injection')	20-09-2019	7.5	App\Mobile\Controller\Zhu antiController.class.php in TuziCMS 2.0.6 has SQL injection via the index.php/Mobile/Zhuanti/g roup?id= substring. CVE ID : CVE-2019-16642		N/A		A-YEJ-TUZI- 141019/341			
Yzmcms	L		I				•			
Yzmcms										
Improper Neutralizatio n of Special Elements in Output Used by a Downstream Component ('Injection')	26-09-2019	5.8	An HTTP Host header injection vulnerability exists in YzmCMS V5.3. A malicious user can poison a web cache or trigger redirections. CVE ID : CVE-2019-16532		N/A		A-YZM- 141019	_		
Cross-Site Request Forgery (CSRF)	21-09-2019	4.3	admin/urlrule/add.html in YzmCMS 5.3 allows CSRF with a resultant denial of service by adding a superseding route. CVE ID : CVE-2019-16678		N/A		A-YZM-YZMC- 141019/343			
zrlog										
zrlog										
Improper Neutralizatio n of Input	20-09-2019	3.5	An issue was discovered in ZrLog 2.1.1. There is a Stored XSS vulnerability in		N/A		A-ZRL-ZRLO- 141019/344			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Patch		NCIIP	C ID		
During Web Page Generation ('Cross-site Scripting')			the article_edit area. CVE ID : CVE-2019-16643							
Zulip							I			
zulip_server										
Uncontrolled Resource Consumption	18-09-2019	4	Zulip used a vulne backt logge send a causin an eff amou	larkdow server b a regular rable to racking. d into th a crafted ng the se ectively nt of CPI rocessing ages.	efore 2. expres exponent A user wer e server message rver to a arbitrar U time a	0.5 sion ntial vho is could ge spend y nd stall	https:, ub.cor p/zuli mmit/ f013b 0c146 1514b 5f2f1b	n/zuli p/co 75797 3be45 a414 oda52	A-ZUL-2 141019	
				D : CVE-						
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	3.5	Zulip server before 2.0.5 incompletely validated the MIME types of uploaded files. A user who is logged into the server could upload files of certain types to mount a stored cross-site scripting attack on other logged-in users. On a Zulip server using the default local uploads backend, the attack is only effective against browsers lacking support for Content-Security-Policy such as Internet Explorer 11. On a Zulip server using the S3 uploads backend, the attack is confined to the origin of the configured S3 uploads hostname and cannot reach		https:, ub.cor p/zuli mmit/ 841df 6b3b0 6f05d f25be3	n/zuli p/co (1195 b9aa2 dabc 72e4a	A-ZUL-2 141019			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	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 Zulip server itself.		
			CVE ID : CVE-2019-16216		
zzzcms				1	
zzzphp					
Unrestricted Upload of File with Dangerous Type	23-09-2019	5	ZZZCMS zzzphp v1.7.2 does not properly restrict file upload in plugins/ueditor/php/contro ller.php?upfolder=news&act ion=catchimage, as demonstrated by uploading a .htaccess or .php5 file. CVE ID : CVE-2019-16720	N/A	A-ZZZ-ZZZP- 141019/347
Improper Input Validation	put 23-09-2019 7.5 Code Execution, because		N/A	A-ZZZ-ZZZP- 141019/348	
			CVE ID : CVE-2019-16722		
			Operating System		
Canonical					
ubuntu_linux					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on	N/A	O-CAN-UBUN- 141019/349

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				107						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID							
			the host.									
			CVE ID : CVE-2019-14835									
Cisco												
nx-os	_	_										
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	25-09-2019	7.2	A vulnerability in a CLI command related to the virtualization manager (VMAN) in Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying Linux operating system with root privileges. The vulnerability is due to insufficient validation of arguments passed to a specific VMAN CLI command on an affected device. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying Linux operating system with root privileges, which may lead to complete system compromise. An attacker would need valid administrator credentials to exploit this vulnerability. CVE ID : CVE-2019-12717		0-CIS-NX-0- 141019/350							
ios_xr Improper Neutralizatio n of Special	25-09-2019	7.2	A vulnerability in a CLI command related to the virtualization manager	N/A	0-CIS-IOS 141019/351							
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 108	6-7 7-8	8-9 9-10							

Weakness	Publish Date	CVSS	Descriptio	on & CVE ID	Pat	ch	NCIIF	'C ID
Elements used in an OS Command ('OS Command Injection')			Series Aggrega Routers could authenticated, to execute arb commands on underlying Lin system with ro The vulnerabil insufficient val arguments pas specific VMAN on an affected attacker who h administrator affected device this vulnerabil including mali the argument of command. A si exploit could a attacker to run commands on underlying op with root privi	isco ASR 9000 ation Services allow an local attacker itrary the nux operating oot privileges. lity is due to lidation of ssed to a CLI command device. An has valid access to an e could exploit lity by cious input as of an affected uccessful allow the n arbitrary the erating system ileges, which omplete system				
ios								
Inadequate Encryption Strength	25-09-2019	5.8	A vulnerability client feature of and IOS XE Sof allow an unau remote attacko modify data the normally have an encrypted of vulnerability is port informati	N/A		0-CIS-I 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 109	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & O	CVE ID	Pat	ch	NCIIP	C ID
			considered when r new requests to ex persistent HTTP connections. An at could exploit this vulnerability by ac man-in-the-middle reading and/or mo data that should no have been sent thr encrypted channel CVE ID : CVE-2019	isting, tacker ting as a e and then odifying ormally ough an				
Improper Link Resolution Before File Access ('Link Following')	25-09-2019	7.2	A vulnerability in t filesystem of Cisco Software could allo authenticated, loca with physical acces affected device to e arbitrary code on t underlying operati (OS) with root priv The vulnerability i insufficient file loc validation. An attac exploit this vulnera placing code in a sp format on a USB de inserting it into an Cisco device. A suc exploit could allow attacker to execute with root privilege underlying OS of the device. CVE ID : CVE-2019	N/A		0-CIS-I(141019		
hyperflex_hx2	220c_af_m5_fi	rmwar	e					
Insufficient Verification of Data	18-09-2019	5	A vulnerability in t statistics collection of Cisco HyperFlex could allow an	N/A		0-CIS-H 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
Authenticity			unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. CVE ID : CVE-2019-12620				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web- based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct clickjacking or other clientside browser attacks. CVE ID : CVE-2019-1975	N/A		0-CIS-H 141019	
hyperflex_hx2	220c_edge_m5	5_firmv				 	
Insufficient Verification	18-09-2019	5	A vulnerability in the statistics collection service	N/A		O-CIS-H	YPE-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 111	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description	& CVE ID	Pat	ch	NCIIF	PC ID
of Data Authenticity			of Cisco HyperFl could allow an unauthenticated attacker to injec values on an affe The vulnerabilit insufficient auth for the statistics service. An attac exploit this vuln sending properly data values to th collection servic affected device. A exploit could allo attacker to cause interface statisti present invalid of CVE ID : CVE-20			141019	/356	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability i based interface o HyperFlex Softw allow an unauth remote attacker cross-frame scri attack on an affe This vulnerabiliti insufficient HTM protection. An ar exploit this vuln directing a user attacker-control page that contain malicious HTML successful explo allow the attacker clickjacking or o clientside brows	N/A		0-CIS-H 141019		
hyperflex_hx2	220c_m5_firm	ware						
CV Scoring Scal								

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Verification of Data Authenticity	18-09-2019	5	A vulnerability in the statistics collection service of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. CVE ID : CVE-2019-12620	N/A	0-CIS-HYPE- 141019/358
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web- based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct clickjacking or other clientside browser attacks.	N/A	O-CIS-HYPE- 141019/359

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				113						

Weakness	Publish Date	CVSS	Description & CVE ID					ch	NCIIP	CID
			CVE I	D : CVE-	·2019-1	975				
hyperflex_hx2	240c_af_m5_fi	rmwar	'e							
Insufficient Verification of Data Authenticity	18-09-2019	5	statistics collection service of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. CVE ID : CVE-2019-12620 A vulnerability in the web-				N/A		O-CIS-H 141019	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web- based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A successful exploit could allow the attacker to conduct				N/A		O-CIS-H 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			client	acking o side bro	wser at					
harring and harring			CVEI	D : CVE-	2019-1	.975				
hyperflex_hx2	240c_m5_firm	ware		1 .1	· .1					
Insufficient Verification of Data Authenticity	18-09-2019	5	A vulnerability in the statistics collection service of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to inject arbitrary values on an affected device. The vulnerability is due to insufficient authentication for the statistics collection service. An attacker could exploit this vulnerability by sending properly formatted data values to the statistics collection service of an affected device. A successful exploit could allow the attacker to cause the web interface statistics view to present invalid data to users. CVE ID : CVE-2019-12620				N/A		0-CIS-H 141019	
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	18-09-2019	4.3	A vulnerability in the web- based interface of Cisco HyperFlex Software could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack on an affected device. This vulnerability is due to insufficient HTML iframe protection. An attacker could exploit this vulnerability by directing a user to an attacker-controlled web page that contains a malicious HTML iframe. A			N/A		0-CIS-H 141019		
CV Scoring Scale	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)	0-1	1-2	2-3	3-4 115	4-5	5-0	0-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to conduct clickjacking or other clientside browser attacks.		
			CVE ID : CVE-2019-1975		
Dlink					
dns-320_firm	ware			T	1
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	16-09-2019	10	The login_mgr.cgi script in D-Link DNS-320 through 2.05.B10 is vulnerable to remote command injection. CVE ID : CVE-2019-16057	N/A	O-DLI-DNS 141019/364
Draytek					
vigor2925_fir	mware				
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	On DrayTek Vigor2925 devices with firmware 3.8.4.3, Incorrect Access Control exists in loginset.htm, and can be used to trigger XSS. NOTE: this is an end-of-life product. This has been solved in v3.8.8.2 and later release firmware. CVE ID : CVE-2019-16533	N/A	0-DRA-VIGO- 141019/365
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	20-09-2019	4.3	On DrayTek Vigor2925 devices with firmware 3.8.4.3, XSS exists via a crafted WAN name on the General Setup screen. NOTE: this is an end-of-life product. This has been solved in v3.8.8.2 and later release firmware	N/A	O-DRA-VIGO- 141019/366
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
		CVE ID : CVE-2019-16534			
t			1		
17-09-2019	7.5	process_http_response in OpenConnect before 8.05 has a Buffer Overflow when a malicious server uses HTTP chunked encoding with crafted chunk sizes. CVE ID : CVE-2019-16239	N/A	O-FED-FEDO- 141019/367	
y_a4_firmware	e				
25-09-2019	10	A broken access control vulnerability in Smart Battery A4, a multifunctional portable charger, firmware version ?<= r1.7.9 allows an attacker to get/reset administrator's password without any authentication. CVE ID : CVE-2019-15068	https://ww w.twcert.or g.tw/subpa ges/ServeT hePublic/p ublic_docu ment_detail s.aspx?lang =en- US&id=45	O-GIG-SMAR- 141019/368	
25-09-2019	7.5	An unsafe authentication interface was discovered in Smart Battery A4, a multifunctional portable charger, firmware version ?<= r1.7.9 . An attacker can bypass authentication without modifying device file and gain web page management privilege. CVE ID : CVE-2019-15069	https://ww w.twcert.or g.tw/subpa ges/ServeT hePublic/p ublic_docu ment_detail s.aspx?lang =en- US&id=46	0-GIG-SMAR- 141019/369	
				l	
27-09-2019	4.3	In libxaac there is a possible information disclosure due	N/A	0-G00-ANDR- 141019/370	
e o t	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	
	t 17-09-2019 25-09-2019 25-09-2019 225-09-2019	Image: space spac	Image: constraint of the second sec	Image: CVE ID : CVE-2019-16534Image: CVE ID : CVE-2019-16534tt17-09-20197.5process_http_response in OpenConnect before 8.05 has a Buffer Overflow when a malicious server uses HTTP chunked encoding with crafted chunk sizes. CVE ID : CVE-2019-16239N/Ay.4_firmwarey.4_firmwarey.5-09-201910A broken access control vulnerability in Smart Battery A4, a multifunctional portable charger, firmware version ?<= r1.7.9 allows an attacker to get/reset administrator's password without any authentication. Interface was discovered in Smart Battery A4, a multifunctional portable charger, firmware version ?<= r1.7.9 An attacker can bypass authentication interface was discovered in Smart Battery A4, a multifunctional portable (charger, firmware version ?<= r1.7.9 An attacker can bypass authentication without modifying device file and gain web page management privilege. CVE ID : CVE-2019-15069https://ww w.twcert.or gtw/subpa ges/ServeT hePublic/p ublic_docu ment_detail s.aspx?lang =en- US&id=4525-09-20194.3In libxaac there is a possible information disclosure dueN/A	

Initialization of Resource27-09-20194.3privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-112204376N/A141019/371Missing Initialization of Resource27-09-20194.3In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-1117626860-GOO-ANDR- 141019/372	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Initialization of Resource27-09-20194.3information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-112204376N/A0-GOO-ANDR- 141019/371Missing Initialization of Resource27-09-20194.3In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-111762686 CVE ID : CVE-2019-9338N/A0-GOO-ANDR- 0-GOO-ANDR- 141019/372Out-of- bounds Read27-09-20195In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote informationN/A0-GOO-ANDR- 141019/373				could lead to information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-113035086		
Missing Initialization of Resource27-09-20194.3information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android Versions: Android- 10Android ID: A-111762686N/AO-GOO-ANDR- 141019/372Out-of- bounds Read27-09-20195In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote informationN/AO-GOO-ANDR- 141019/372	Initialization	27-09-2019	4.3	information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-112204376	N/A	O-GOO-ANDR- 141019/371
Out-of- bounds Read27-09-20195possible out of bounds read due to a missing bounds check. This could lead to remote informationN/A0-GOO-ANDR- 141019/373	Initialization	27-09-2019	4.3	information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-111762686	N/A	O-GOO-ANDR- 141019/372
		27-09-2019	5	possible out of bounds read due to a missing bounds check. This could lead to remote information	N/A	O-GOO-ANDR- 141019/373

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				118						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 111214770		
			CVE ID : CVE-2019-9341		
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 111214470 CVE ID : CVE-2019-9342	N/A	0-GOO-ANDR- 141019/374
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 112050983 CVE ID : CVE-2019-9343	N/A	0-G00-ANDR- 141019/375
Out-of- bounds Write	27-09-2019	6.8	In libstagefright, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote code execution with no additional execution	N/A	0-G00-ANDR- 141019/376

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				119						

L

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIPC				
			privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-128433933							
			CVE ID : CVE-2019-9346							
Improper Input Validation	27-09-2019	7.1	In libstagefright, there is a possible resource exhaustion due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-128431761 CVE ID : CVE-2019-9348	N/A		0-G00-/ 141019				
Out-of- bounds Read	27-09-2019	4.3	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-123024201 CVE ID : CVE-2019-9353	N/A		0-G00-/ 141019				
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	N/A		0-G00- 141019				
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID		ch	NCIIPC ID	
			Product: AndroidVersions: Android-10Android ID: A- 115903122				
			CVE ID : CVE-2019-9355				
Improper Input Validation	27-09-2019	7.5	In Bluetooth, there is a possible deserialization error due to missing string validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-109838537 CVE ID : CVE-2019-9365	N/A		0-G00-ANDR- 141019/380	
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 112106425 CVE ID : CVE-2019-9367	N/A		0-G00-ANDR- 141019/381	
Out-of- bounds Read	27-09-2019	2.1	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-	N/A		0-G00-ANDR- 141019/382	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patcl	h	NCIIF	PC ID
			10Android ID: A-79883568				
			CVE ID : CVE-2019-9368				
Improper Input Validation	27-09-2019	7.1	In libskia, there is a possible crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-132782448	N/A		0-GO0- 141019	
			CVE ID : CVE-2019-9372				
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 117569833	N/A		0-G00- 141019	
			CVE ID : CVE-2019-9387				
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure in the Bluetooth service with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 117567437	N/A		0-GOO- 141019	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)			122				

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	CID
			CVE ID : CVE-						
Out-of- bounds Read	27-09-2019	5	In Bluetooth, a possible out o due to a missi check. This co remote denial no additional privileges nee interaction is exploitation. H AndroidVersio 10Android ID	of bounds ng bound ould lead t l of service execution eded. User not neede Product: ons: Andr : A-11756	s o e with ed for oid- 57058	N/A		0-G00- 141019	
Out-of- bounds Read	27-09-2019	5	In Bluetooth, a possible out o due to a missi check. This co remote denial no additional privileges nee interaction is exploitation. F AndroidVersio 10Android ID CVE ID : CVE-	N/A		0-G00- 141019			
Inadequate Encryption Strength	27-09-2019	4.3	The Print Service is susceptible to man in the middle attacks due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-115635664 CVE ID : CVE-2019-9399			N/A		0-G00- 141019	
N/A	27-09-2019	4.3	In libavc there is a possible			N/A		0-G00-	ANDR-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-112380157 CVE ID : CVE-2019-9408		141019/389
N/A	27-09-2019	4.3	In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-112204443 CVE ID : CVE-2019-9410	N/A	O-GOO-ANDR- 141019/390
N/A	27-09-2019	4.3	In libavc there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-112204845 CVE ID : CVE-2019-9411	N/A	0-GOO-ANDR- 141019/391
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to	N/A	0-GOO-ANDR- 141019/392
CV Scoring Scal	-				

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				12/						

Weakness	Publish Date	CVSS	Description & CVE ID				ch	NCIIF	PC ID
			remote inforr disclosure wi execution pri User interacti needed for ex Product: And Android-10A 111935831						
			CVE ID : CVE	-2019-9	413				
N/A	27-09-2019	4.3	In libstagefright there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-111805098 CVE ID : CVE-2019-9415			N/A		0-GOO- 141019	
N/A	27-09-2019	4.3	In libstagefright there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-111804142 CVE ID : CVE-2019-9416			N/A		0-GOO- 141019	
Out-of- bounds Read	27-09-2019	2.1	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution			N/A		0-G00- 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 125	4-5	5-6	6-7	7-8	8-9	9-10

125	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-111450079		
			CVE ID : CVE-2019-9417		
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 111407544	N/A	0-GOO-ANDR- 141019/396
			CVE ID : CVE-2019-9419		
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 111214766	N/A	O-GOO-ANDR- 141019/397
	CVE ID : CVE-2019-9422				
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User	N/A	O-GOO-ANDR- 141019/398
CV Scoring Scale	-				

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				126						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-110846194		
			CVE ID : CVE-2019-9425		
Use After Free	27-09-2019	4	In Bluetooth, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure with heap information written to the log with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 109755179	N/A	0-G00-ANDR- 141019/399
			CVE ID : CVE-2019-9431		
Out-of- bounds Read	27-09-2019	5	In Bluetooth, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure in the Bluetooth server with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A- 80546108	N/A	0-G00-ANDR- 141019/400
			CVE ID : CVE-2019-9432		
Improper Input Validation	27-09-2019	4.3	In libvpx, there is a possible information disclosure due to improper input validation. This could lead to remote information disclosure with no additional execution	N/A	0-G00-ANDR- 141019/401

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				127						

Г

Out-of- bounds Read27-09-20194In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remete information written to the log with System execution privileges needed. User interaction is not needed for exploitation. Product: Android UD: A-80479354N/A0-GOO-ANDR 141019/402Out-of- bounds Read27-09-20194In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information not interaction is not needed for exploitation. Product: Android UD: A-80432895N/A0-GOO-ANDR 141019/402Out-of- bounds Read27-09-20192.1In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to nocal information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android VERSIONS: Android- 10Android ID: A-80432895N/A0-GOO-ANDR 141019/402Out-of- bounds Read27-09-20192.1In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to IOCAL Information disclosure with no additional execution privileges needed. UserN/A0-GOO-ANDR 141019/403Out-of- bounds Read27-09-20195In Bluetooth, there is a possible out of bounds read due to a nincorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. UserN/A0-GOO-ANDR 141019/404	Weakness	Publish Date	CVSS	Description & CVE ID		Patch	NCIIP	CID
Out-of- bounds Read27-09-20194In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with heap information written to the log with System execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-80432895N/AO-GOO-ANDR 141019/402Out-of- bounds Read27-09-20194In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android- local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android- local information disclosure with no additional execution privileges needed. UserN/A0-GOO-ANDR lation/4004Out-of- bounds Read27-09-20195In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no addition. Product: AndroidVersions: Android- 10Android ID: A-80146682N/A0-GOO-ANDR lation/404Out-of- bounds Read27-09-20195In Bluetooth, there is a possible out of bounds read due to a incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. UserN/A0-GOO-ANDR lation/404				interaction is needed for exploitation. Product: AndroidVersions: Android	-			
Out-of- bounds Read27-09-20194a special possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with heap information written to the 				CVE ID : CVE-2019-9433	3			
Out-of- bounds Read27-09-20192.1In Bluetooth, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android- 10Android ID: A-80146682N/AO-GOO-ANDR 141019/403Out-of- bounds Read27-09-20195In Bluetooth, there is a possible out of bounds read due to an incorrect bounds check. This could lead to no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android- 10Android ID: A-801466820-GOO-ANDR 141019/403Out-of- bounds Read27-09-20195In Bluetooth, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. UserN/A0-GOO-ANDR 141019/404		27-09-2019	4	possible out of bounds readue to a missing bounds check. This could lead to remote information disclosure with heap information written to the log with System execution privileges needed. User interaction is not needed to exploitation. Product: AndroidVersions: Android 10Android ID: A-8043289	e N/A for d- 95	Ą		
Out-of- bounds Read27-09-20195possible out of bounds read due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. UserN/A0-GOO-ANDR 141019/404		27-09-2019	2.1	possible out of bounds readue to a missing bounds check. This could lead to local information disclosu with no additional execution privileges needed. User interaction is not needed to exploitation. Product: AndroidVersions: Android 10Android ID: A-8014668 CVE ID : CVE-2019-9435	ire ion for d- 32	Ą		
		27-09-2019	5	possible out of bounds rea due to an incorrect bound check. This could lead to remote denial of service w no additional execution	ls N/A	A		
CV Scoring Scale (CVSS) 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	-	e 0-1	1-2	2-3 3-4 4-5 5-	-6 6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				170						

Weakness	Publish Date	CVSS	Description	on & CVE	ID	Pat	ch	NCIIF	PC ID
			interaction is exploitation. AndroidVersi 10Android ID	Product: ons: And	lroid-				
			CVE ID : CVE	2019-9	462				
Intel	L		L			<u> </u>		I	
e5-4628l_firm	nware								
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition microprocess (R) DDIO cach and RDMA man authenticated potentially en information d adjacent acces CVE ID : CVE	ors usin ne alloca ay allow l user to nable par lisclosur ss.	g Intel tion an tial e via	https:/ w.intel /conte ww/us securif center sory/in sa- 00290	l.com ent/w s/en/ ty- /advi ntel-	0-INT- 141019	
e5-4657l_firm	nware								
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition microprocess (R) DDIO cach and RDMA ma authenticated potentially en information d adjacent acces	https:/ w.intel /conte ww/us securit center sory/it sa- 00290	l.com ent/w s/en/ ty- /advi ntel-	0-INT-) 141019			
e7-2850_firm	ware								
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184			https:/ w.intel /conte ww/us securit center sory/in sa- 00290	l.com ent/w s/en/ ty- /advi ntel-	0-INT- 141019	
e7-2870_firm	ware								
CV Scoring Scale	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Concurrent Execution					
using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-E7-2- 141019/408
e7-2880_firmv	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-2- 141019/409
e7-2890_firmv	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-2- 141019/410
e7-4860_firmv	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa-	O-INT-E7-4- 141019/411
CV Scoring Scale (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
Condition')			CVE I	D : CVE-	2019-1	1184	00290	.html		
e7-4870_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) DI and R authe poten inforr adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				//ww l.com ent/w s/en/ ty- ty- r/advi ntel-	0-INT-I 141019	
e7-4880_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) DI and R authe poten inforr adjace	e condition processor DIO cach DMA ma nticated tially en nation d ent acces D : CVE-	ors usin e alloca y allow user to able par isclosur ss.	ng Intel ation y an rtial re via	https:, w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	O-INT-F 141019	
e7-4890_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) DI and R authe poten inforr adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184		https:, w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	O-INT-F 141019		
e7-8850_firm	ware									
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial			https://ww w.intel.com /content/w ww/us/en/ security- center/advi		0-INT-F 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Synchronizat			information disclosure via	sory/intel-		
ion ('Race			adjacent access.	sa-		
Condition')			CVE ID : CVE-2019-11184	00290.html		
e7-8857_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-8- 141019/416	
e7-8895_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-8- 141019/417	
e5-2623_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/418	
e5-2628l_firn	nware					
Concurrent Execution using Shared	16-09-2019	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://ww w.intel.com /content/w	O-INT-E5-2- 141019/419		
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				127						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronizat ion ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	ww/us/en/ security- center/advi sory/intel- sa- 00290.html	
e5-2630_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/420
e5-2630l_firn	nware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/421
e5-2637_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/422
e5-2640_firm	ware			1	1
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	D Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spec microprocessors using (R) DDIO cache allocatio and RDMA may allow an authenticated user to potentially enable parti information disclosure adjacent access. CVE ID : CVE-2019-11	Intel w.intel.com on /content/w n ww/us/en/ security- ial center/advi via sory/intel- sa-	0-INT-E5-2- 141019/423
e5-2643_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spec microprocessors using (R) DDIO cache allocatio and RDMA may allow an authenticated user to potentially enable parti information disclosure adjacent access. CVE ID : CVE-2019-11	Intel w.intel.com on /content/w n ww/us/en/ security- ial center/advi via sory/intel- sa-	O-INT-E5-2- 141019/424
e5-2648l_firm	iware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spec microprocessors using (R) DDIO cache allocatio and RDMA may allow at authenticated user to potentially enable parti information disclosure adjacent access. CVE ID : CVE-2019-11	Intel w.intel.com on /content/w n ww/us/en/ security- ial center/advi via sory/intel- sa-	O-INT-E5-2- 141019/425
e5-2650_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race	16-09-2019	2.9	A race condition in spec microprocessors using (R) DDIO cache allocatio and RDMA may allow an authenticated user to potentially enable parti information disclosure adjacent access.	Intel w.intel.com on /content/w n ww/us/en/ security- ial center/advi	0-INT-E5-2- 141019/426
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
Condition')			CVE I	D : CVE-	2019-1	1184	00290	.html		
e5-2650l_firm	nware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) DI and R authe poten inforr adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				//ww l.com ent/w s/en/ ty- ty- r/advi ntel-	0-INT-I 141019	-
e5-2658_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184			https:, w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- ty- r/advi ntel-	O-INT-F 141019	-	
e5-2660_firm	ware		•							
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) Dl and R authe poten inforr adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184		https:, w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- ty- r/advi ntel-	0-INT-F 141019		
e5-2667_firm	ware									
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial			https://ww w.intel.com /content/w ww/us/en/ security- center/advi		0-INT-I 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4 135	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Synchronizat			information disclosure via	sory/intel-		
ion ('Race			adjacent access.	sa-		
Condition')			CVE ID : CVE-2019-11184	00290.html		
e5-2670_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/431	
e5-2680_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/432	
e5-2683_firm	ware				1	
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/433	
e5-2687w_fir	mware					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	O-INT-E5-2- 141019/434		
CV Scoring Scal	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
126										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Resource with Improper Synchronizat ion ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	ww/us/en/ security- center/advi sory/intel- sa- 00290.html		
e5-2690_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/435	
e5-2695_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/436	
e5-2697_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-E5-2- 141019/437	
e5-2698_firm	ware				1	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spec microprocessors using I (R) DDIO cache allocatio and RDMA may allow an authenticated user to potentially enable partia information disclosure v adjacent access. CVE ID : CVE-2019-111	ntel w.intel.com n /content/w ww/us/en/ security- al center/advi ria sory/intel- sa-	0-INT-E5-2- 141019/438	
e5-2699_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spec microprocessors using I (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure v adjacent access. CVE ID : CVE-2019-111	ntel w.intel.com n /content/w ww/us/en/ security- al center/advi ria sory/intel- sa-	O-INT-E5-2- 141019/439	
e5-4610_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spec microprocessors using I (R) DDIO cache allocatio and RDMA may allow ar authenticated user to potentially enable partia information disclosure v adjacent access. CVE ID : CVE-2019-111	ntel w.intel.com n /content/w ww/us/en/ security- al center/advi ria sory/intel- sa-	O-INT-E5-4- 141019/440	
e5-4620_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race	16-09-2019	2.9	A race condition in spec microprocessors using I (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure wa adjacent access.	ntel w.intel.com on /content/w ww/us/en/ security- al center/advi	O-INT-E5-4- 141019/441	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Patch		NCIIP	C ID
Condition')			CVE II	D : CVE-	2019-1	1184	00290).html		
e5-4627_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				https://w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	0-INT-I 141019	-
e5-4640_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184		https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html		O-INT-F 141019	-		
e5-4650_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184			https:, w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	O-INT-I 141019		
e5-4655_firm	ware								1	
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial			https://ww w.intel.com /content/w ww/us/en/ security- center/advi		0-INT-F 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Synchronizat ion ('Race Condition')			information disclosure via adjacent access. CVE ID : CVE-2019-11184	sory/intel- sa- 00290.html		
e5-4660_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-4- 141019/446	
e5-4667_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-4- 141019/447	
e5-4669_firm	ware				I	
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-4- 141019/448	
e7-4809_firm	ware			I	I	
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://ww w.intel.com /content/w	O-INT-E7-4- 141019/449	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 with Improper Synchronizat ion ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	ww/us/en/ security- center/advi sory/intel- sa- 00290.html				
e7-4820_firm	e7-4820_firmware							
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-4- 141019/450			
e7-4830_firm	ware							
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-4- 141019/451			
e7-4850_firm	ware							
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-4- 141019/452			
e7-8870_firm	ware				I			
CV Scoring Scale (CVSS) 0-1 1-2 2-3 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 Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-E7-8- 141019/453	
e7-8880_firm	ware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-8- 141019/454	
e7-88801_firm	nware					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E7-8- 141019/455	
e7-8890_firm	ware			·		
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa-	O-INT-E7-8- 141019/456	

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Patch		NCIIP	C ID
Condition')			CVE I	D : CVE-	2019-1	1184	00290).html		
e7-8891_firm	ware		<u> </u>							
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				https: w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	O-INT-I 141019	
e7-8893_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184			https:/ w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	0-INT-F 141019		
3106_firmwa	re									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184			https:/ w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	0-INT-3 141019		
4109t_firmwa	are		1							
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial			https://ww w.intel.com /content/w ww/us/en/ security- center/advi		0-INT-4 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4 1/13	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Synchronizat ion ('Race Condition')			information disclosure via adjacent access. CVE ID : CVE-2019-11184	sory/intel- sa- 00290.html		
4110_firmwa	re				L	
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-4110- 141019/461	
4114t_firmwa	are					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-4114- 141019/462	
4116_firmwa	re					
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-4116- 141019/463	
4116t_firmwa	are					
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://ww w.intel.com /content/w	O-INT-4116- 141019/464	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

g Scale S)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
				144					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronizat ion ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	ww/us/en/ security- center/advi sory/intel- sa- 00290.html	
5118_firmwa	re				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-5118- 141019/465
5119t_firmwa	are				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-5119- 141019/466
5120t_firmwa	are				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	0-INT-5120- 141019/467
6126_firmwa	re				<u> </u>
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE I	D Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spe microprocessors using (R) DDIO cache allocati and RDMA may allow a authenticated user to potentially enable part information disclosure adjacent access. CVE ID : CVE-2019-11	Intel w.intel.com ion /content/w in ww/us/en/ security- ial center/advi via sory/intel- sa-	O-INT-6126- 141019/468
6126t_firmwa	ire				·
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spe microprocessors using (R) DDIO cache allocation and RDMA may allow a authenticated user to potentially enable part information disclosure adjacent access. CVE ID : CVE-2019-11	Intel w.intel.com ion /content/w in ww/us/en/ security- ial center/advi via sory/intel- sa-	0-INT-6126- 141019/469
6130_firmwa	re				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in spe microprocessors using (R) DDIO cache allocati and RDMA may allow a authenticated user to potentially enable part information disclosure adjacent access. CVE ID : CVE-2019-11	Intel w.intel.com ion /content/w in ww/us/en/ security- ial center/advi via sory/intel- sa-	O-INT-6130- 141019/470
6130t_firmwa	ire				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race	16-09-2019	2.9	A race condition in spe microprocessors using (R) DDIO cache allocati and RDMA may allow a authenticated user to potentially enable part information disclosure adjacent access.	Intel w.intel.com ion /content/w in ww/us/en/ security- ial center/advi	0-INT-6130- 141019/471
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5	5-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pa	tch	NCIIF	PC ID
Condition')			CVE I	D : CVE-	2019-1	1184	00290).html		
6138_firmwa	re								1	
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) D and R authe poten inforn adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				//ww l.com ent/w s/en/ ty- ty- r/advi ntel-	0-INT-6 141019	
e5-2403_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) D and R authe poten inforn adjace	e conditi oprocess DIO cach DMA ma nticated nticated ntially en nation d ent acces D : CVE-	ors usin ne alloca ay allow user to able par isclosur ss.	ng Intel ntion r an rtial re via	https: w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	O-INT-I 141019	
e5-2407_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) D and R authe poten inforn adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184		https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html		0-INT-H 141019		
e5-2420_firm	ware									
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	micro (R) D and R authe	e conditi oprocess DIO cach DMA ma nticated itially en	ors usin le alloca ay allow user to	ng Intel Ition Yan	https:/ w.inte /conte ww/u securi center	l.com ent/w s/en/ ty-	0-INT-I 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4 147	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronizat ion ('Race Condition')			information disclosure via adjacent access. CVE ID : CVE-2019-11184	sory/intel- sa- 00290.html	
e5-2430_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/476
e5-2430l_firm	nware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific https: microprocessors using Intel (R) DDIO cache allocation /cont and RDMA may allow an ww/u authenticated user to secur potentially enable partial cente information disclosure via adjacent access. sa- CVE ID : CVE-2019-11184 0029		O-INT-E5-2- 141019/477
e5-2440_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/478
e5-2450_firm	ware			1	I
Concurrent Execution using Shared	16-09-2019	2.9 microprocessors using Intel w.intel.com		https://ww w.intel.com /content/w	O-INT-E5-2- 141019/479
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Descripti	on & CVE	ID	Pat	tch	NCIIF	PC ID
Resource with Improper Synchronizat ion ('Race Condition')			authe poter infor adjac	and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				s/en/ ty- /advi ntel- .html		
e5-2450l_firn	nware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) D and F authe poter inform adjac	e condition process DIO cach DMA ma enticated ntially er mation d ent acce D : CVE	ors usin ne alloca ay allow l user to nable pan lisclosur ss.	g Intel ation an rtial re via	https:/ w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- /advi ntel-	0-INT-I 141019	
e5-2470_firm	ware								L	
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html		0-INT-I 141019	
e5-2697a_firr	nware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184		https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html		O-INT-I 141019			
e5-2699a_firr	nware									
CV Scoring Scal	e 0-1	1-2	2-3	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 Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/483
e5-4603_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-4- 141019/484
e5-4607_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-4- 141019/485
e5-1620_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access.	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa-	O-INT-E5-1- 141019/486
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 150	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
Condition')			CVE I	D : CVE-	2019-1	1184	00290).html		
e5-1630_firm	ware									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) DI and R auther poten inform adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184				//ww l.com ent/w s/en/ ty- ty- r/advi ntel-	0-INT-I 141019	
e5-1650_firm	ware		1						l	
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) DI and R auther poten inform adjace	e conditi processe DIO cach DMA ma nticated tially en nation d ent acces D : CVE-	ors usir ae alloca ay allow user to able pa isclosun ss.	ng Intel ation y an rtial re via	https:, w.inte /conte ww/u securi center sory/i sa- 00290	l.com ent/w s/en/ ty- '/advi ntel-	O-INT-I 141019	-
e5-1660_firm	ware		<u> </u>						[
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	micro (R) DI and R auther poten inform adjace	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184		https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html		O-INT-F 141019		
e5-1680_firm	ware									
Concurrent Execution using Shared Resource with Improper	16-09-2019	2.9	micro (R) DI and R auther	e conditi process DIO cach DMA ma nticated tially en	ors usir le alloca ly allow user to	ng Intel ation 7 an	https:/ w.inte /conte ww/u securi center	l.com ent/w s/en/ ty-	0-INT-I 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4 151	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronizat ion ('Race Condition')			information disclosure via adjacent access. CVE ID : CVE-2019-11184	sory/intel- sa- 00290.html	
e5-2603_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/491
e5-2608l_firm	nware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/492
e5-2609_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/493
e5-2618l_firm	nware				
Concurrent Execution using Shared	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation	https://ww w.intel.com /content/w	O-INT-E5-2- 141019/494
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				152						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronizat ion ('Race Condition')			and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	ww/us/en/ security- center/advi sory/intel- sa- 00290.html	
e5-2620_firm	ware				
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	16-09-2019	2.9	A race condition in specific microprocessors using Intel (R) DDIO cache allocation and RDMA may allow an authenticated user to potentially enable partial information disclosure via adjacent access. CVE ID : CVE-2019-11184	https://ww w.intel.com /content/w ww/us/en/ security- center/advi sory/intel- sa- 00290.html	O-INT-E5-2- 141019/495
intenogroup					
eg200_firmwa	are				
Information Exposure Through Discrepancy	16-09-2019	4.3	Inteno EG200 EG200- WU7P1U_ADAM03.16.4- 190226_1650 routers have a JUCI ACL misconfiguration that allows the "user" account to extract the 3DES key via JSON commands to ubus. The 3DES key is used to decrypt the provisioning file provided by Adamo Telecom on a public URL via cleartext HTTP. CVE ID : CVE-2019-13140	N/A	O-INT-EG20- 141019/496
keeper					
keeper k5_firmware					
-	19-09-2019	7.2	On Keeper K5 20.1.0.25 and 20.1.0.63 devices, remote code execution can occur by inserting an SD card containing a file named	N/A	O-KEE-K5_F- 141019/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			zskj_script_run.sh that		
			executes a reverse shell.		
			CVE ID : CVE-2019-16398		
Linux					
linux_kernel					
Information Exposure	23-09-2019	5	In the Linux kernel before 5.2.14, rds6_inc_info_copy in net/rds/recv.c allows attackers to obtain sensitive information from kernel stack memory because tos and flags fields are not initialized.	N/A	0-LIN-LINU- 141019/498
			CVE ID : CVE-2019-16714		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	7.5	An issue was discovered in net/wireless/nl80211.c in the Linux kernel through 5.2.17. It does not check the length of variable elements in a beacon head, leading to a buffer overflow. CVE ID : CVE-2019-16746	N/A	0-LIN-LINU- 141019/499
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in Linux kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code. CVE ID : CVE-2019-14814	N/A	O-LIN-LINU- 141019/500
Buffer Copy without Checking Size of Input ('Classic Buffer	20-09-2019	7.2	There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a	N/A	O-LIN-LINU- 141019/501
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	ו	NCIIPO	D
Overflow')			denial of service(system crash) or possibly execute arbitrary code.				
Out-of- bounds Write	19-09-2019	7.2	CVE ID : CVE-2019-14816 An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system. CVE ID : CVE-2019-14821			O-LIN-LI 141019/	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on	N/A		0-LIN-LI 141019/	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 host. CVE ID : CVE-2019-14835						
Loop with Unreachable Exit Condition ('Infinite Loop')	18-09-2019	5	An issue was discovered in the Linux kernel before 5.0.4. The 9p filesystem did not protect i_size_write() properly, which causes an i_size_read() infinite loop and denial of service on SMP systems. CVE ID : CVE-2019-16413	N/A		0-LIN-LINU 141019/50			
Improper Initialization	27-09-2019	5	In the Linux kernel before 4.17, hns_roce_alloc_ucontext in drivers/infiniband/hw/hns/ hns_roce_main.c does not initialize the resp data structure, which might allow attackers to obtain sensitive information from kernel stack memory, aka CID- df7e40425813. CVE ID : CVE-2019-16921	N/A		0-LIN-LINU 141019/50			
mi									
xiaomi_millet	t_firmware								
Unrestricted Upload of File with Dangerous Type	18-09-2019	5.8	A malicious file upload vulnerability was discovered in Xiaomi Millet mobile phones 1-6.3.9.3. A particular condition involving a man-in-the- middle attack may lead to partial data leakage or malicious file writing. CVE ID : CVE-2019-15843	https://sec. xiaomi.com /post/152		O-MI-XIAO- 141019/506			
nxp									
kinetis_k8x_firmware									
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 Authenticati on	24-09-2019	4.6	On NXP Kinetis KV1x, Kinetis KV3x, and Kinetis K8x devices, Flash Access Controls (FAC) (a software IP protection method for execute-only access) can be defeated by leveraging a load instruction inside the execute-only region to expose the protected code into a CPU register. CVE ID : CVE-2019-14239	N/A	0-NXP-KINE- 141019/507
kinetis_kv1x_	firmware				
Improper Authenticati on	24-09-2019	4.6	On NXP Kinetis KV1x, Kinetis KV3x, and Kinetis K8x devices, Flash Access Controls (FAC) (a software IP protection method for execute-only access) can be defeated by leveraging a load instruction inside the execute-only region to expose the protected code into a CPU register. CVE ID : CVE-2019-14239	N/A	O-NXP-KINE- 141019/508
kinetis_kv3x_	firmware				
Improper Authenticati on	24-09-2019	On NXP Kinetis KV1x, Kinetis KV3x, and Kinetis K8x devices, Flash Access Controls (FAC) (a software IP protection method for execute-only access) can be		N/A	O-NXP-KINE- 141019/509
			CVE ID - CVE-2017-14239		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
157										

Weakness	Publish Date	CVSS	Description	n & CVE ID	Pa	tch	NCIIP	PC ID	
Opensuse	I	<u> </u>					<u> </u>		
leap									
Concurrent Execution using Shared Resource with Improper Synchronizat ion ('Race Condition')	25-09-2019	6.8	It was discover was a ECDSA ti the libgcrypt20 cryptographic Version affecte 1.7.6-2+deb9u 2+deb8u4. Ver 1.8.5-2 and 1.6 CVE ID : CVE-2	ming attack ir) library. d: 1.8.4-5, 3, and 1.6.3- sions fixed: .3-2+deb8u7.	N/A		O-OPE- 141019		
Redhat									
virtualization									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overfle found, in versio 2.6.34 to 5.2.x, Linux kernel's functionality the virtqueue buffe logged the buffe during migratio privileged guess pass descriptor length to the he migration is un could use this f increase their p the host. CVE ID : CVE-2	ons from in the way vhost nat translates ers to IOVs, fer descriptors on. A st user able to rs with invalid ost when iderway, law to privileges on	N/A		O-RED- 141019	-	
enterprise_lin	nux						<u> </u>		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap- overflow in Lin versions up to, in the marvell driver in Linux allows local use denial of servic crash) or possi	, N/A		O-RED- 141019			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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.		
			CVE ID : CVE-2019-14814		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code. CVE ID : CVE-2019-14816	N/A	O-RED-ENTE- 141019/513
Out-of- bounds Write	19-09-2019	7.2	An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system. CVE ID : CVE-2019-14821	N/A	O-RED-ENTE- 141019/514
Insufficient Session Expiration	17-09-2019	2.1	A flaw was found in FreeIPA versions 4.5.0 and later. Session cookies were retained in the cache after logout. An attacker could	https://bug zilla.redhat. com/show_ bug.cgi?id= CVE-2019-	O-RED-ENTE- 141019/515
CV Scoring Scal					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				150						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			abuse this flaw if they obtain previously valid session cookies and can use this to gain access to the session. CVE ID : CVE-2019-14826	14826	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-09-2019	7.2	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host. CVE ID : CVE-2019-14835	N/A	O-RED-ENTE- 141019/516
messaging_re	altime_grid				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in Linux kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system crash) or possibly execute arbitrary code. CVE ID : CVE-2019-14814	N/A	O-RED-MESS- 141019/517
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-09-2019	7.2	There is heap-based buffer overflow in kernel, all versions up to, excluding 5.3, in the marvell wifi chip driver in Linux kernel, that allows local users to cause a denial of service(system	N/A	O-RED-MESS- 141019/518
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crash) or possibly execute		
			arbitrary code.		
			CVE ID : CVE-2019-14816		
Schneider-ele					
modicon_prei	mium_firmwa	re			
Improper Handling of Exceptional Conditions	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580 (firmware versions prior to V2.90), Modicon M340 (firmware versions prior to V3.10), Modicon Premium (all versions), Modicon Quantum (all versions), which could cause a possible denial of service when reading invalid data from the controller.	https://ww w.schneider - electric.com /en/downlo ad/docume nt/SEVD- 2019-134- 11/	O-SCH-MODI- 141019/519
			CVE ID : CVE-2019-6809		
Improper Handling of Exceptional Conditions	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists Modicon M580 (firmware version prior to V2.90), Modicon M340 (firmware version prior to V3.10), Modicon Premium (all versions), and Modicon Quantum (all versions), which could cause a possible denial of service when reading specific coils and registers in the controller over Modbus. CVE ID : CVE-2019-6828	https://ww w.schneider - electric.com /en/downlo ad/docume nt/SEVD- 2019-134- 11/	O-SCH-MODI- 141019/520
modicon_qua	ntum firmwa	re			
Improper Handling of Exceptional	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists in Modicon M580	O-SCH-MODI- 141019/521	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			(firmware versions prior to V2.90), Modicon M340 (firmware versions prior to V3.10), Modicon Premium (all versions), Modicon Quantum (all versions), which could cause a possible denial of service when reading invalid data from the controller. CVE ID : CVE-2019-6809	electric.com /en/downlo ad/docume nt/SEVD- 2019-134- 11/	
Improper Handling of Exceptional Conditions	17-09-2019	7.8	A CWE-248: Uncaught Exception vulnerability exists Modicon M580 (firmware version prior to V2.90), Modicon M340 (firmware version prior to V3.10), Modicon Premium (all versions), and Modicon Quantum (all versions), which could cause a possible denial of service when reading specific coils and registers in the controller over Modbus. CVE ID : CVE-2019-6828	https://ww w.schneider - electric.com /en/downlo ad/docume nt/SEVD- 2019-134- 11/	O-SCH-MODI- 141019/522
modicon_m34	0_firmware				
Improper Check for Unusual or Exceptional Conditions	17-09-2019	7.8	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists in BMXNOR0200H Ethernet / Serial RTU module (all firmware versions) and Modicon M340 controller (all firmware versions), which could cause denial of service when truncated SNMP packets on port 161/UDP	https://ww w.schneider - electric.com /en/downlo ad/docume nt/SEVD- 2019-225- 03/	O-SCH-MODI- 141019/523

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				162						

Г

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			are received by the device.						
			CVE ID : CVE-2019-6813						
modicon_quar	ntum_140noe	77101	_firmware	I	L				
Improper Check for Unusual or Exceptional Conditions	17-09-2019	5	An Improper Check for Unusual or Exceptional Conditions (CWE-754) vulnerability exists in Modicon Quantum 140 NOE771x1 version 6.9 and earlier, which could cause denial of service when the module receives an IP fragmented packet with a length greater than 65535 bytes. The module then requires a power cycle to recover.		O-SCH-MODI- 141019/524				
			CVE ID : CVE-2019-6811						
modicon_qua	ntum_140noe	77111	_firmware						
Improper Check for Unusual or Exceptional Conditions	17-09-2019	5	An Improper Check for Unusual or Exceptional Conditions (CWE-754) vulnerability exists in Modicon Quantum 140 NOE771x1 version 6.9 and earlier, which could cause denial of service when the module receives an IP fragmented packet with a length greater than 65535 bytes. The module then requires a power cycle to recover. CVE ID : CVE-2019-6811	https://ww w.schneider - electric.com /en/downlo ad/docume nt/SEVD- 2019-253- 02/	O-SCH-MODI- 141019/525				
hmigto_firmw	hmigto_firmware								
Improper Check for Unusual or	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions	https://ww w.schneider -	O-SCH-HMIG- 141019/526				
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exceptional Conditions			vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. CVE ID : CVE-2019-6833	electric.com /ww/en/do wnload/doc ument/SEV D-2019- 225-01	
hmigxo_firmv	vare				
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. CVE ID : CVE-2019-6833	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 225-01	O-SCH-HMIG- 141019/527
hmigxu_firmv	ware			_	
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO,	https://ww w.schneider - electric.com /ww/en/do wnload/doc	O-SCH-HMIG- 141019/528
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-1 0

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel.	ument/SEV D-2019- 225-01				
			CVE ID : CVE-2019-6833					
hmiscu_firmware								
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. CVE ID : CVE-2019-6833	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 225-01	O-SCH-HMIS- 141019/529			
hmisto_firmw	vare							
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO,	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 225-01	O-SCH-HMIS- 141019/530			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	D	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			a temp HMI w frames attack comm	oorary f /hen a h s is rece stops, t	ich coul reeze of igh rate vived. W he buffe e proces l.	the of hen the ered				
			CVE II	D : CVE-	2019-6	833				
hmistu_firmw	are		•							
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	Check Except vulner Magel versio HMIST HMIGT XBTGT HMIGT a temp HMI w frames attack comm the HM	for Unu tional C rability is HMI H ns of - H TO, XBT TUX, HM T, XBTG XU), wh porary f yhen a h s is rece stops, t ands ar MI pane	T, HMIG ich coul reeze of igh rate eived. W he buffe e proces	ns all , IGTU, IMISTU, XO, d cause The of hen the ered ssed by	https:, w.schr - electri /ww/ wnloa ument D-201 225-0	neider c.com en/do d/doc c/SEV 9-	O-SCH-1 141019	
xbtgh_firmwa	ire									
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of			https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 225-01		0-SCH-XBTG- 141019/532		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frames is received. When attack stops, the buffered commands are processed the HMI panel.		
			CVE ID : CVE-2019-6833		
xbtgt_firmwa	re				
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU HMIGTUX, HMISCU, HMIS XBTGT, XBTGT, HMIGXO, HMIGXU), which could can a temporary freeze of the HMI when a high rate of frames is received. When a attack stops, the buffered commands are processed the HMI panel. CVE ID : CVE-2019-6833	TU, electric.com /ww/en/do unent/SEV D-2019- the 225-01 by	0-SCH-XBTG- 141019/533
bmxnor0200l	h_firmware				
Incorrect Authorizatio n	17-09-2019	6.5	CWE-284: Improper Accest Control vulnerability exist in BMXNOR0200H Ethern / Serial RTU module (all firmware versions), which could cause the execution commands by unauthoriz users when using IEC 60870-5-104 protocol. CVE ID : CVE-2019-6810	ts https://ww https://ww w.schneiden - electric.com of /en/downlo ad/docume nt/SEVD- 2019-225- 03/	0-SCH-BMXN- 141019/534
Improper Check for Unusual or Exceptional	17-09-2019	7.8	A CWE-754: Improper Che for Unusual or Exceptiona Conditions vulnerability exists in BMXNOR0200H Ethernet / Serial RTU		0-SCH-BMXN- 141019/535
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-	-6 6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS		Descripti	on & CVE	ID	Pat	ch	NCII	PC ID
Conditions			version M340 firmv could when packed are re	module (all firmware versions) and Modicon M340 controller (all firmware versions), which could cause denial of service when truncated SNMP packets on port 161/UDP are received by the device. CVE ID : CVE-2019-6813 A CWE-754: Improper Check for Unusual or Exceptional				cume /D- 225-		
Improper Check for Unusual or Exceptional Conditions	17-09-2019	5	A CW for U Cond exists Ether modu versid disco conno unus IEC 6 are re on po	Æ-754: I	mprope r Except Inerabil NOR020 rial RTU rmware ich could of activ vhen an h numbe 104 pac by the m /TCP.	r Check ional ity 00H d cause ve er of ekets odule	https:/ w.schr - electri /en/do ad/do nt/SEV 2019-2 03/	c.com ownlo cume /D-	O-SCH- 141019	
sick							1			
fx0-gent0000	0_firmware									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	5	SICK FX0-GPNT00000 and FX0-GENT00000 devices through 3.4.0 have a Buffer Overflow CVE ID : CVE-2019-14753		https://ww w.sick.com/ medias/SCA -2019- 002.pdf?con text=bWFzd GVyfGNvbn RlbnR8MjE 5MDk1fGF wcGxpY2F0 aW9uL3Bk Znxjb250Z W50L2g3Yy 9oNDEvMT		0-SIC-F 141019			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				AzMDY0NjA zNTI1NDIu cGRmfDJlZT VmZjJmYzY wYmQ10D QyZDBmMj A00Tc3ZDB jMmY1YzZk YzUzNzI0M WI00GIy0T E00TllY2VI YjJhNzUzYT E	
fx0-gpnt0000	0_firmware				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	24-09-2019	5	SICK FX0-GPNT00000 and FX0-GENT00000 devices through 3.4.0 have a Buffer Overflow CVE ID : CVE-2019-14753	https://ww w.sick.com/ medias/SCA -2019- 002.pdf?con text=bWFzd GVyfGNvbn RlbnR8MjE 5MDk1fGF wcGxpY2F0 aW9uL3Bk Znxjb250Z W50L2g3Yy 9oNDEvMT AzMDY0NjA zNTI1NDIu cGRmfDJIZT VmZjJmYzY wYmQ10D QyZDBmMj A00Tc3ZDB jMmY1YzZk YzUzNzI0M WI00GIyOT E00TIIY2VI YjJhNzUzYT	O-SIC-FX0 141019/538

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				169						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
				Е		
ST						
stm32f4_firm	ware					
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. CVE ID : CVE-2019-14238	N/A	0-ST-STM3- 141019/539	
stm32f7_firm	ware			1		
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. CVE ID : CVE-2019-14238	N/A	0-ST-STM3- 141019/540	
stm32h7_firm	iware					
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. CVE ID : CVE-2019-14238	N/A	O-ST-STM3- 141019/541	
stm32l0_firm	ware				1	
Improper	24-09-2019	4.6	On STMicroelectronics	N/A	O-ST-STM3-	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 170	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticati on			STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. CVE ID : CVE-2019-14238		141019/542
stm32l1_firm	ware				
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. CVE ID : CVE-2019-14238	N/A	0-ST-STM3- 141019/543
stm32l4_firm	ware				
Improper Authenticati on	24-09-2019	4.6	On STMicroelectronics STM32F7 devices, Proprietary Code Read Out Protection (PCROP) (a software IP protection method) can be defeated with a debug probe via the Instruction Tightly Coupled Memory (ITCM) bus. CVE ID : CVE-2019-14238	N/A	O-ST-STM3- 141019/544
Supermicro					
x10drt-ps_firm	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in	N/A	O-SUP-X10D- 141019/545
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers of use captured credentials t connect virtual USB device to the server managed by BMC. CVE ID : CVE-2019-1664	to es the			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X products, a client's access privileges may be transferred to a different client that later has the sa socket file descriptor number. In opportunistic circumstances, an attacket can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-1665	me r N/A		O-SUP-X 141019	
x10drt-pt_firm	nware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems if the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers of use captured credentials to connect virtual USB device to the server managed by BMC.	of N/A		0-SUP-> 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-10

1	7	2

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/548
x10drt-p_firm	ware		CVE ID : CVE-2019-10030		
xiourep_mm	IWAIC				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/549
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D- 141019/550
CV Scoring Scale	a		2.2 2.4 4.5 5.6		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				173						

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	:h	NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10drt-pibf_fi	irmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-> 141019	
x10drt-pibq_f	firmware		0.0.1.1144.1140				
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP->	X10D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC			141019	/553
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege 20 Management	0-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x10drw-i_firmwa	are						
Use of Hard- coded 20 Credentials	0-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	0-1	1-2	2-3 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 the server managed by the BMC.			
			CVE ID : CVE-2019-16649			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/556	
			CVE ID : CVE-2019-16650			
x10dsc+_firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/557	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D- 141019/558	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650					
x10qbl-ct_firm	nware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-X10Q- 141019/559			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10Q- 141019/560			
x10qbl_firmware								
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X10Q- 141019/561
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X12 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X10Q- 141019/562
x10qrh+_firm	iware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca	n N/A	O-SUP-X10Q- 141019/563
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10Q- 141019/564
x10sae_firmw	are				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/565
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different		O-SUP-X10S- 141019/566
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16650				
x10sat_firmwa	are		On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16650		
x10sdd-16c-f	firmware			I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/569
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10S- 141019/570
x10sdd-f_firm	iware			I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10S- 141019/571
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 181	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10S- 141019/572
x10sde-df_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/573
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	C ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	/574
x10sdv-12c+-	tln4f_firmwa	re					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			0-SUP-> 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		0-SUP-> 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID					ch	NCIIP	CID
			devices to the server managed by the BMC.							
				D : CVE-		6650				
x10sdv-12c-tl	n∕lf⊥ firmwa		CVEI		2019-1	0030				
x105uv-12t-u		e	On Cu		o II11 I	110	[[
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				N/A		O-SUP-2 141019	
x10sdv-12c-tl	ln4f_firmware	•								
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in				N/A		0-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649	s he			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X1 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	ne N/A		0-SUP-X 141019	
x10sdv-16c+-	tln4f_firmwa	re					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by the BMC.	n N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/582
			CVE ID : CVE-2019-16650		
x10sdv-16c-tl	n4f+_firmwa	re			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/583
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10S- 141019/584
CV Scoring Scale	e 0-1		2-3 3-4 4-5 5-6	6-7 7-8	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				106						

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10sdv-16c-tl	ln4f_firmware	è					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-> 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-> 141019	
x10sdv-2c-7tp	p4f_firmware					I	
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		0-SUP->	(10S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 187	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	escriptio	on & CVE	ID	Pat	tch	NCIIP	PC ID
Credentials			encrypt authent the virt allows credent transfer media o use cap connect to the s BMC.	tion an tication tual me capture tials an rred ov devices tured o tured o t virtua	n proble edia serv e of BM0 nd data ver virtu s. Attack credent al USB d manage	ems in vice C nal ers can ials to evices d by the			141019	9/587
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				N/A		O-SUP-2 141019	
x10sdv-2c-tln	2f_firmware		L							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices				N/A		0-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/590
			CVE ID : CVE-2019-16650		
x10sdv-2c-tp4	4f_firmware	_			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/591
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10S- 141019/592
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	h	NCIIP	CID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10sdv-2c-tp8	Bf_firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x10sdv-4c+-tl	n4f_firmware	e	I				
	e o i						

Weakness	Publish Date	CVSS	Description & CVE ID	Patcl	h	NCIIP	C ID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			0-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-X 141019	
x10sdv-4c+-t	p4f_firmware			1			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A		0-SUP-X 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10S- 141019/598
x10sdv-4c-7t	p4f firmware		CVEID. CVE-2019-10030		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/599
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-X10S- 141019/600
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
	0.6. 6		CVE ID : CVE-2019-16650				
x10sdv-4c-tln			On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16650		
x10sdv-4c-tln	4f_firmware				<u> </u>
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/603
Improper Privilege Management x10sdv-6c+-t	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	0-SUP-X10S- 141019/604
			On Supermicro H11 H12		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	0-SUP-X10S- 141019/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10S- 141019/606
x10sdv-6c-tln	4f_firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/607
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	/608
x10sdv-7tp4f	firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-> 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		0-SUP-> 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			devices to the server managed by the BMC.							
				D : CVE-						
x10sdv-7tp8f	firmware		GTEI	2.012						
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede transt media use ca conne to the BMC.	permicr X9, X10, acts, a co ption an ntication rtual me s captur ntials an ferred ov a devices aptured o ect virtua eserver a	and X1 mbinati d n proble edia serv e of BM0 d data ver virtu s. Attack credent al USB d manage	1 ion of ems in vice C al ters can ials to evices d by the	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Su produ privil transi client socke numb circun can si virtua then o devic mana	permicr icts, a cli eges may ferred to that late t file des t file des per. In op mstances mply co al media connect es to the ged by th D : CVE-	o X10 a ent's ac y be a differ er has th criptor portuni s, an atta nnect to service, virtual U server he BMC.	nd X11 cess rent ne same istic acker o the and JSB	N/A		O-SUP-2 141019	
x10sdv-8c+-li	121_III mware		0.0		. 114.4 .	110				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of N/A encryption and authentication problems in			O-SUP-2 141019				
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-X 141019	
x10sdv-8c-tln	4f+_firmware	9		1			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Pat	tch	NCIIF	C ID	
			CVE ID :	CVE-2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	products privilege transferr client tha socket fil number. circumst can simp virtual m then com devices t managed	micro X10 a , a client's ac s may be ed to a differ at later has th e descriptor In opportuni ances, an atta ly connect to edia service, nect virtual U o the server by the BMC. CVE-2019-1	cess rent he same astic acker o the and JSB	N/A		O-SUP-2 141019	
x10sdv-8c-tln	4f_firmware					I		L	
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, products encryptic authentic the virtua allows ca credentia transferr media de use captu connect v to the sen BMC.	micro H11, H X10, and X17 , a combination on and cation problec al media serv opture of BM0 als and data ed over virtu evices. Attack ured credention virtual USB d cver manageo CVE-2019-1	1 con of ems in vice C nal ters can tials to evices d by the	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker		N/A		0-SUP-2 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3	-4 4-5 199	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				100						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	•	NCIIPC	ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10sdv-f_firm	iware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-X1 141019/	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-X1 141019/	
x10sdv-tln4f_	firmware						
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	(O-SUP-X1	10S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Credentials							
			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	/621
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x10sdv-tp8f_fin	rmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-2 141019	
CV Scoring Scale	0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/624
			CVE ID : CVE-2019-16650		
x10sl7-f_firm	ware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.N/ACVE ID : CVE-2019-16649Image Service M1000000000000000000000000000000000000		O-SUP-X10S- 141019/625
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	0-SUP-X10S- 141019/626
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	ch	NCIIP	PC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10sla-f_firm	ware	_					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-X 141019	
x10sld-f_firm	ware		L				
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X10S- 141019/629
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X12 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X10S- 141019/630
x10sld-hf_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca	n N/A	O-SUP-X10S- 141019/631
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/632
v10alo df finn			CVE ID : CVE-2019-16650		
x10sle-df_firm	nware		0 . 0		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/633
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-X10S- 141019/634
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID		ch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16650				
x10sle-f_firm	ware		On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16650		
x10sle-hf_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	0-SUP-X10S- 141019/637
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	0-SUP-X10S- 141019/638
x10slh-f_firm	ware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10S- 141019/639
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10S- 141019/640
x10sll+-f_firm	iware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/641
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIF	PC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	0/642
x10sll-f_firmv	vare						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		O-SUP-2 141019	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	De	escriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			devices manage							
			CVE ID							
v10all a firm			CVEID	. CVE	2019-1	0030				
x10sll-s_firm	ware		0		- II11 I	110	[
Use of Hard- coded Credentials	20-09-2019	5	transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		N/A		O-SUP-2 141019			
			CVE ID	: CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic			N/A		O-SUP-X 141019		
x10sll-sf_firm	ware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			l on of	N/A		0-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	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 virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X10S- 141019/648
x10slm+-f_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car use captured credentials to connect virtual USB devices to the server managed by th BMC.		O-SUP-X10S- 141019/649
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

2	1	1
2	т	T.

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/650
			CVE ID : CVE-2019-16650		
x10slm+-ln4f	firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/651
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10S- 141019/652
CV Scoring Scale					

(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
CV Scoring Scale	0.1		2.2				c -			0.40

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID	
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.					
x10slm-f_firm	Mana		CVE ID : CVE-2019-16650					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-X 141019		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	N/A		O-SUP-X10S- 141019/654	
x10slx-f_firmv	ware							
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-X	X10S-	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 213	6-7	7-8	8-9	9-10	

Credentials			Description & CVE ID		ch	NCIIPC ID		
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	9/655	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019		
x10sra-f_firmv	ware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A	N/A		O-SUP-X10S- 141019/657	
CV Scoring Scale	0-1	1-2	2-3 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 the server managed by the BMC.			
			CVE ID : CVE-2019-16649			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/658	
			CVE ID : CVE-2019-16650			
x10sra_firmw	are					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/659	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10S- 141019/660	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	PC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10srd-f_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-X10S- 141019/662	
x10srg-f_firm	ware			L			
	2 0.1						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X10S- 141019/663
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X12 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X10S- 141019/664
x10srh-cf_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca	N/A	0-SUP-X10S- 141019/665
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10S- 141019/666
v10crh cln4f	firmwara		CVE ID : CVE-2019-16650		
x10srh-cln4f_	nrmware		On Companying U11, U12		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/667
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-X10S- 141019/668
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10sri-f_firmv	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description 8	Pat	ch	NCIIP	CID	
			CVE ID : CVE-20					
x10srl-f_firm	ware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		N/A		O-SUP-X 141019	
Improper Privilege Management x10srm-f_firm	20-09-2019 aware	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic		N/A		O-SUP-3 141019	
			On Supermicro H	H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC		N/A		O-SUP-X 141019	
CV Scoring Scale	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10S- 141019/674
x10srm-tf_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10S- 141019/675
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10S-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	C ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	/676
x10srw-f_firm	iware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			O-SUP-≯ 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		0-SUP-> 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			devices to the server managed by the BMC.							
			CVE ID : CVE-2019-16650							
x11dac_firmv	varo		CVE ID : CVE-2019-16650							
			On Su	nermicr	o H11 F	412	[
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		ion of ems in vice C N/A nal ters can ials to levices		on of ms in ice al ers can als to evices		K11D- /679	
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		N/A		O-SUP-X 141019			
x11dai-n_firm	nware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		O-SUP-X11D- 141019/681		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	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 virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X11D- 141019/682
x11ddw-l_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car use captured credentials to connect virtual USB devices to the server managed by the BMC.		O-SUP-X11D- 141019/683
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D- 141019/684
			CVE ID : CVE-2019-16650		
x11ddw-nt_fi	rmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/685
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11D- 141019/686
CV Scoring Scale	o		22 24 45 56		

(CV33)				225						
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patcl	h	NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11dgo-t_firm	iware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-X 141019	
x11dgq_firmw			0- 0- 1111				
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-X	X11D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descripti	on & CVE	ID	Pat	ch	NCIIP	PC ID
Credentials			products, a co encryption ar authenticatio the virtual mo allows captur credentials ar transferred o media device use captured connect virtu to the server BMC. CVE ID : CVE	nd n proble edia serv re of BM0 nd data ver virtu s. Attack credenti al USB d manageo	ems in vice C al ers can ials to evices d by the			141019	/689
Improper Privilege Management	20-09-2019	7.5	On Supermice products, a cl privileges ma transferred to client that lat socket file des number. In op circumstance can simply co virtual media then connect devices to the managed by t	N/A		0-SUP-2 141019			
x11dpff-sn_fin	rmware								
Use of Hard- coded Credentials	20-09-2019	5	On Supermice M11, X9, X10 products, a co encryption ar authenticatio the virtual me allows captur credentials ar transferred o media device use captured connect virtu	N/A		0-SUP-2 141019			
CV Scoring Scale	e 0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D- 141019/692
			CVE ID : CVE-2019-16650		
x11dpfr-s_firm	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.N/ACVE ID : CVE-2019-16649I		O-SUP-X11D- 141019/693
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X11D- 141019/694
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		
x11dpfr-sn_fi	rmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/695
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11D- 141019/696
x11dpg-ot-cpu	u_firmware			1	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-X11D- 141019/697
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11D- 141019/698
x11dpg-qt_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X11D- 141019/699
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D- 141019/700
x11dpg-sn_fir	mware		CVE ID : CVE-2019-16650		
viinh8-211 ¹¹¹	niwale		On Supermicro H11, H12,		
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/701
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X11D- 141019/702
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16650				
x11dph-i_firm	Iwale		On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16650		
x11dph-t_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/705
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11D- 141019/706
x11dph-tq_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	0-SUP-X11D- 141019/707
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11D- 141019/708
x11dpi-n_firm	nware			1	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/709
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019,	/710
x11dpi-nt_firm	mware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-X 141019,	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		O-SUP-X 141019,	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	I	Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			devices to the server managed by the BMC.							
				D : CVE-						
v11dpl i firm			CVEI	D.CVE-	2019-1	0030				
x11dpl-i_firm	ware		0.0		. 1111 1	110	[
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede transf media use ca conne	permicr X9, X10, acts, a co ption an ntication rtual me s capture ntials an ferred ov a devices optured o ect virtua	and X1 mbinati d n proble edia serv e of BM0 d data ver virtu s. Attack credenti al USB d	1 on of ems in vice C nal ers can ials to evices	N/A		O-SUP-2 141019	
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649On Supermicro X10 and X11products, a client's accessprivileges may betransferred to a differentclient that later has the samesocket file descriptornumber. In opportunisticcircumstances, an attackercan simply connect to thevirtual media service, andthen connect virtual USBdevices to the servermanaged by the BMC.CVE ID : CVE-2019-16650		N/A		O-SUP-X 141019			
x11dps-re_fir	mware									
Use of Hard- coded Credentials	20-09-2019	5	nroducts a combination of N/A			0-SUP-X 141019				
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	'C ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-2 141019	
x11dpt-b_firm	nware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.			O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D- 141019/718
			CVE ID : CVE-2019-16650		
x11dpt-bh_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/719
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11D- 141019/720
CV Scoring Scal					

(CVSS)	·			2.	. 0					5 10
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	•		ch	NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11dpt-l_firm	iware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-X 141019	
x11dpt-ps_fir	mware						
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-X	(11D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 239	6-7	7-8	8-9	9-10

	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIF	PC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	0/723
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x11dpu-v_firm	nware			-			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-2 141019	
CV Scoring Scale	e 0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11D- 141019/726
			CVE ID : CVE-2019-16650		
x11dpu-x_firr	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/727
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	0-SUP-X11D- 141019/728
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7	-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	'C ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11dpu-xll_fir	rmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649	N/A n ne		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X12 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	e N/A		O-SUP-2 141019	
x11dpu-z+_fir	mware		l				
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X11D- 141019/731
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X1 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		0-SUP-X11D- 141019/732
x11dpu-ze+_f	irmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca	N/A n	0-SUP-X11D- 141019/733
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11D- 141019/734
x11dpu_firmv	ware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/735
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-X11D- 141019/736
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11dpx-t_firm	iware		CVE ID . CVE-2019-10050				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description &	Pat	ch	NCIIP	C ID	
			CVE ID : CVE-201					
x11dsc+_firm	ware							
Use of Hard- coded Credentials	 On Supermicro H11 M11, X9, X10, and X products, a combinate encryption and authentication probethe virtual media set allows capture of BN credentials and data transferred over virtual use captured credent connect virtual USB to the server manage BMC. CVE ID : CVE-2019 		X11 ination of oblems in service BMC ata virtual tackers can lentials to SB devices aged by the	N/A		O-SUP-X 141019		
Improper Privilege Management	20-09-2019 ware	7.5	CVE ID : CVE-201 On Supermicro X1 products, a client' privileges may be transferred to a d client that later ha socket file descrip number. In oppor circumstances, an can simply connect virtual media serv then connect virtu devices to the serv managed by the B CVE ID : CVE-201	N/A		O-SUP-X 141019		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro Ha M11, X9, X10, and products, a combi- encryption and authentication pro- the virtual media allows capture of	N/A		O-SUP-X 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11D- 141019/742
x11dsn-ts_firm	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11D- 141019/743
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	CID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	/744
x11dsn-tsq_fi	rmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			O-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		O-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
				es to the ged by tl						
				D : CVE-						
x11opi-cpu_fi	rmuaro		CVEI	D.CVL-	2019-1	0030				
	Illiwale		On Cu		o II11 I	110	[[
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			N/A		O-SUP-2 141019		
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			N/A		0-SUP-2 141019		
x11qph+_firm	iware									
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry	permicr X9, X10, icts, a co ption an	and X11 mbinati d	l on of	N/A		0-SUP-2 141019	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	h	NCIIPC ID		
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649	s ne				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X1 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	ne N/A		O-SUP-> 141019	•	
x11sca-f_firm	ware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC.	N/A in		O-SUP-≯ 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10	

250	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2019-16649			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	0-SUP-X11S- 141019/752	
x11sca-w_firm	nware					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the	N/A	O-SUP-X11S- 141019/753	
			BMC. CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access			
Improper Privilege Management CV Scoring Scale	20-09-2019	7.5	privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11S- 141019/754	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				251						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.					
			CVE ID : CVE-2019-16650					
x11sca_firmw	are		0.0.0.0.000	1				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/755			
			CVE ID : CVE-2019-16649					
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11S- 141019/756			
x11scd-f_firmware								
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X11S-			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 252	6-7 7	7-8 8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIF	PC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	0/757
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x11sch-f_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-2 141019	
CV Scoring Scale	e 0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/760
			CVE ID : CVE-2019-16650		
x11sch-ln4f_f	irmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/761
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X11S- 141019/762
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIP	PC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11scl-f_firmv	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-2 141019	
x11scl-if_firm	ware		1				
CV Scoring Scale			2-3 3-4 4-5 5-6	6-7	7-8		9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-X11S- 141019/765
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	0-SUP-X11S- 141019/766
x11scl-ln4f_fi	rmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car	N/A	0-SUP-X11S- 141019/767
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/768
x11scm-f_firm	iware		CVE ID : CVE-2019-16650		
XIISCIII-I_IIIII	Iware		On Supermicro H11, H12,		
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	0-SUP-X11S- 141019/769
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X11S- 141019/770
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11scm-ln8f_1	firmwaro		CVE ID : CVE-2019-10050				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description 8	Pat	ch	NCIIP	C ID	
			CVE ID : CVE-20					
x11scw-f_firm	iware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H M11, X9, X10, and products, a comb encryption and authentication put the virtual media allows capture of credentials and d transferred over media devices. An use captured created connect virtual U to the server man BMC.	N/A		O-SUP-X 141019		
Improper Privilege Management	20-09-2019 _firmware	7.5	CVE ID : CVE-20 On Supermicro X products, a client privileges may be transferred to a c client that later h socket file descri number. In oppor circumstances, an can simply connect virtual media ser then connect virt devices to the ser managed by the b CVE ID : CVE-20	N/A		O-SUP-X 141019		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H M11, X9, X10, and products, a comb encryption and authentication pu the virtual media allows capture of	N/A		O-SUP-X 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	0-SUP-X11S- 141019/776
x11sdd-8c-f_f	irmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/777
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSS	Des	cription & CVE	ID	Pat	tch	NCIIP	C ID
Privilege Management			products privilege transferr client tha socket fil number. circumst can simp virtual m then con devices t managed CVE ID :			141019	/778		
x11sds-12c_fi	rmware								
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		N/A		0-SUP-X 141019		
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB			N/A		0-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2		3-4 4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	•				Pat	ch	NCIIP	CID
			devices to the server managed by the BMC.							
			CVE ID : CVE-2019-16650							
v11ada 16a fi			CVEI	D.CVE-	2019-1	0030				
x11sds-16c_fi	rinware		Ore Cre		- 1111 1	110	[
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.			N/A		O-SUP-2 141019		
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649On Supermicro X10 and X11products, a client's accessprivileges may betransferred to a differentclient that later has the samesocket file descriptornumber. In opportunisticcircumstances, an attackercan simply connect to thevirtual media service, andthen connect virtual USBdevices to the servermanaged by the BMC.CVE ID : CVE-2019-16650		N/A		O-SUP-X 141019			
x11sds-8c_fir	mware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		O-SUP-2 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-X 141019	
x11spa-t_firm	iware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIF	PC ID
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	produ privile transf client socket numb circum can sin virtua then c device manag	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			N/A		O-SUP-2 141019	
x11spa-tf_firm	nware									
Use of Hard- coded Credentials	20-09-2019	5	M11, 2 produ encryj auther the vir allows creden transf media use ca conne to the BMC.	transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the		N/A		0-SUP-2 141019		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker			N/A		0-SUP-2 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4 264	4-5	5-6	6-7	7-8	8-9	9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				264						

Weakness	Publish Date	CVSS	Description & CVE ID		ch	NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16650				
x11spg-tf_firm	nware		On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		О-SUР-Х 141019	
			CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-X 141019	-
x11sph-nctf_f	irmware						
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-X	X11S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	CID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	/791
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			0-SUP-X 141019	
x11sph-nctpf	_firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		0-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/794
			CVE ID : CVE-2019-16650		
x11spi-tf_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/795
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	0-SUP-X11S- 141019/796
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	'C ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11spl-f_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x11spm-f_firm	nware		1				
CV Scoring Scale		1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	CID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems if the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers of use captured credentials to connect virtual USB device to the server managed by BMC. CVE ID : CVE-2019-1664	of n N/A can co es the		O-SUP-X 141019,	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X products, a client's access privileges may be transferred to a different client that later has the sa socket file descriptor number. In opportunistic circumstances, an attacke can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-1665	me r N/A		O-SUP-X 141019,	
x11spm-tf_fir	mware			l			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems if the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers of	of n N/A		O-SUP-X 141019,	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-	6 6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	NCIIPC ID	
			use captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/802
			CVE ID : CVE-2019-16650		
x11spm-tpf_fi	irmware			1	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/803
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-X11S- 141019/804
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
4.4			CVE ID : CVE-2019-16650				
x11spw-ctf_fi	iniware		On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16650		
x11spw-tf_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/807
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11S- 141019/808
x11sri-if_firm	ware			L	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X11S- 141019/809
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11S- 141019/810
x11srl-f_firm	ware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/811
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	CID
Privilege Management			privile transfe client socket numbe circum can sin virtua then c device manag	cts, a cli eges may erred to that late that late file des er. In op nstances mply con stances nply con l media onnect es to the ged by th D : CVE-	y be a differ er has th scriptor portunt s, an atta nnect to service, virtual U server he BMC.	rent ne same istic acker o the and JSB			141019	/812
x11srm-f_firm	nware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.				N/A		0-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB			N/A		0-SUP-X 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
			devices to the server managed by the BMC.							
			CVE ID : CVE-2019-16650							
x11srm-vf_fir	muaro		CVEI	D.CVL-	2019-1	0030				
X1151III-V1_III	IIIwale		On Su		o II11 I	110				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			N/A		O-SUP-2 141019	-	
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			N/A		0-SUP-2 141019		
x11ssd-f_firm	ware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in				N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			0-SUP-2 141019	
x11sse-f_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car use captured credentials to connect virtual USB devices to the server managed by the BMC.			O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16649							
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/820					
			CVE ID : CVE-2019-16650							
x11ssh-ctf_firmware										
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/821					
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X11S- 141019/822					
CV Scoring Scale	0									

()				777						
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x11ssh-f_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-X 141019	_
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-X 141019,	-
x11ssh-gf-158	85_firmware						
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-X	(11S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 278	6-7	7-8	8-9	9-10

Credentials							
			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	/825
Improper Privilege 2 Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x11ssh-gf-1585	5l_firmware						
Use of Hard- coded Z Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-2 141019	
CV Scoring Scale	0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	0-SUP-X11S- 141019/828
			CVE ID : CVE-2019-16650		
x11ssh-gtf-15	85_firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/829
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	0-SUP-X11S- 141019/830
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	h NCIIPC ID
			number. In opportunistic circumstances, an attacke can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-1665	er e l	
x11ssh-gtf-15	851_firmware	•			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers use captured credentials connect virtual USB device to the server managed by BMC. CVE ID : CVE-2019-1664	of in N/A can to ces the	O-SUP-X11S- 141019/831
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X products, a client's access privileges may be transferred to a different client that later has the sa socket file descriptor number. In opportunistic circumstances, an attacke can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-1665	ame Pr 1	0-SUP-X11S- 141019/832
x11ssh-ln4f_fi	rmware				
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5	-6 6-7	7-8 8-9 9-1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X11S- 141019/833
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X11S- 141019/834
x11ssh-tf_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car	N/A	O-SUP-X11S- 141019/835
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.			
			CVE ID : CVE-2019-16649			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/836	
x11ssi-ln4f_fi	rmware		CVE ID : CVE-2019-16650			
X1155I-III41_III	IIIware		On Supermicro H11, H12,			
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11products, a combination ofencryption andauthentication problems inthe virtual media serviceallows capture of BMCcredentials and datatransferred over virtualmedia devices. Attackers canuse captured credentials toconnect virtual USB devicesto the server managed by theBMC.CVE ID : CVE-2019-16649		0-SUP-X11S- 141019/837	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-X11S- 141019/838	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIPC ID	
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
x11ssl-cf firm	ware		CVE ID : CVE-2019-16650				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descriptio	on & CVE ID	Pat	ch	NCIIP	CID
			CVE ID : CVE-	2019-16650				
x11ssl-f_firm	ware				<u> </u>			
Use of Hard- coded Credentials	20-09-2019	5	use captured of connect virtua to the server r BMC.	and X11 mbination of d n problems in dia service e of BMC d data ver virtual . Attackers can credentials to al USB devices managed by the	N/A		O-SUP-2 141019	
Improper Privilege Management x11ssl-nf_firm	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic		N/A		O-SUP-2 141019	
X1155I-III_III II	Iwale							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC		N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X11S- 141019/844
x11ssl_firmwa	are				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/845
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X11S-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7·	-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID						
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		141019/84								
x11ssm-f_firmware													
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			O-SUP-X11S- 141019/847							
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	O-SUP-X11S- 141019/848								
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10						

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIPC ID					
			devices to the server										
			managed by the BMC.										
			CVE ID : CVE-2019-16650										
x11ssm_firmware On Supermicro H11, H12,													
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede trans media use ca conne	apermicr X9, X10, acts, a co ption an entication rtual me s captur ntials an ferred ov a devices aptured o ect virtua	and X12 mbinati d n proble dia serv e of BM0 d data ver virtu s. Attack credenti al USB d	1 on of ems in vice C nal ers can ials to evices	N/A		0-SUP-X11S- 141019/849				
			CVE I	D : CVE-	2019-1	6649							
Improper Privilege Management	20-09-2019	7.5	produ privil transi client socke numb circun can si virtua then o devic mana	ipermicr acts, a cli eges may ferred to that late t file des per. In op mstances mply co al media connect es to the ged by th D : CVE-	ent's ac y be a differ er has th criptor portuni s, an atta nnect to service, virtual U server he BMC.	cess rent le same stic acker o the and JSB	N/A		O-SUP-X11S- 141019/850				
x11ssw-4tf_fi	rmware												
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		0-SUP-X11S- 141019/851					
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	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 virtual media serv allows capture of BMC credentials and data transferred over virtu media devices. Attack use captured credenti connect virtual USB d to the server managed BMC. CVE ID : CVE-2019-1	C al ers can als to evices d by the		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and products, a client's accur privileges may be transferred to a differ client that later has the socket file descriptor number. In opportuni circumstances, an atta can simply connect to virtual media service, then connect virtual U devices to the server managed by the BMC. CVE ID : CVE-2019-1	cess ent le same stic acker the and JSB	'A	O-SUP-X11S- 141019/852
x11ssw-f_firm	iware					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, F M11, X9, X10, and X11 products, a combinati encryption and authentication proble the virtual media serv allows capture of BM0 credentials and data transferred over virtu media devices. Attack use captured credenti connect virtual USB d to the server managed BMC.	l on of ms in rice C N/ al ers can als to evices	ΎΑ	O-SUP-X11S- 141019/853
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X11S- 141019/854
			CVE ID : CVE-2019-16650		
x11ssw-tf_firm	nware	1	r	1	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X11S- 141019/855
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	0-SUP-X11S- 141019/856
CV Scoring Scale	e 0-1		2-3 3-4 4-5 5-6		

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
200										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16650		
x9da7/e_firm	ware		On Supermiero H11 H12		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DA- 141019/857
x9dai_firmwa	re				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DA- 141019/858

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
291										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
x9dal-3/i_firm	nware	1									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DA- 141019/859						
x9dax-7/i(t)f_firmware											
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DA- 141019/860						
x9dax-7/if-hf	t_firmware										
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service	N/A	O-SUP-X9DA- 141019/861						
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10						

Weakness	Publish Date	CVSS	Description & CVE ID) Pa	tch	NCIIP	CID			
			allows capture of BMC credentials and data transferred over virtual media devices. Attacker use captured credential connect virtual USB dev to the server managed b BMC.	rs can s to vices by the						
v0dh2/; (tn)f	firmurano		CVE ID : CVE-2019-166	649						
x9db3/i-(tp)f_firmware On Supermicro H11, H12,										
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination encryption and authentication problem the virtual media servic allows capture of BMC credentials and data transferred over virtual media devices. Attacker use captured credential connect virtual USB dev to the server managed b BMC. CVE ID : CVE-2019-166	n of is in re N/A rs can s to rices by the		0-SUP-X 141019				
x9dbl-3/i(f)_f	irmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H1 M11, X9, X10, and X11 products, a combination encryption and authentication problem the virtual media servic allows capture of BMC credentials and data transferred over virtual media devices. Attacker use captured credential connect virtual USB dev to the server managed b	n of s in re N/A rs can s to rices		O-SUP-≯ 141019				
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5	5-6 6-7	7-8	8-9	9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMC.		
			CVE ID : CVE-2019-16649		
x9dbs-f(-2u)_	firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC.	n n ne	O-SUP-X9DB- 141019/864
			CVE ID : CVE-2019-16649		
x9dbu-3/if_fi	rmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649	ne	O-SUP-X9DB- 141019/865
x9dr/i-f_firm	ware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of	N/A	O-SUP-X9DR- 141019/866
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7·	-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIPC ID
			encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.			
			CVE ID : CVE-2019-16649			
x9dr3/i-ln4f+	firmware					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-X9DR- 141019/867
x9dr7-jln4f_fi	rmware					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A		O-SUP-X9DR- 141019/868
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.						
			CVE ID : CVE-2019-16649						
x9dr7/e-ln4f	firmware								
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X9DR- 141019/869				
vodu7/a tfu f	in manana		CVE ID : CVE-2019-16649						
x9dr7/e-tf+_f Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X9DR- 141019/870				
			CVE ID : CVE-2019-16649						
x9drd-7ln4f_series_firmware									
CV Scoring Scal									

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
296										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/871
x9drd-c(n)t+	firmware			<u> </u>	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/872
x10dru-i+_fir	mware			I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	0-SUP-X10D- 141019/873
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/874
x10dru-x_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/875
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	-8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIF	PC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	9/876
x10dru-xll_fir	mware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		0-SUP-2 141019	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
				es to the ged by t						
				D : CVE-						
x10drw-it_fir	mwara		CVEI	DICVE	2019-1	0030				
x10ulw-lt_lill	lliware		0		. 1111 1	110	[[
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede trans media use ca conne	apermicr X9, X10, acts, a co ption an intication rtual me s captur ntials ar ferred ov a devices aptured ect virtua	and X1 ombinati d n proble edia serv e of BM nd data ver virtu s. Attack credent al USB d	1 ion of ems in vice C nal ters can ials to evices	N/A		O-SUP-X 141019	
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			N/A		0-SUP-X 141019		
x10drw-nt_fir	rmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		0-SUP-X 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-2 141019	
x10qbl-4_firm	iware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10Q- 141019/884
x10qbl-4ct_fi	rmware		CVEID. CVE-2019-10030		
ALUQUI-TCL_III	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10Q- 141019/885
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10Q- 141019/886
CV Scoring Scale	o		2.2 2.4 4.5 5.6	6-7 7-8	8-0 0.10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				202						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	า	NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
a1sa2-2750f_1	firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-4 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-A 141019	-
a1sai-2550f_f	irmware						
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-A	A1SA-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 3 03	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	/889
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-4 141019	
a1sai-2750f_f	irmware		<u> </u>			<u> </u>	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		0-SUP-A 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-A1SA- 141019/892
			CVE ID : CVE-2019-16650		
a1sam-2550f	_firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-A1SA- 141019/893
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	0-SUP-A1SA- 141019/894
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIP	'C ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
a1sam-2750f	firmware			-			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-4 141019	-
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-4 141019	
a1sri-2358f_fi	irmware						
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-A1SR- 141019/897
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-A1SR- 141019/898
a1sri-2558f_f	irmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-A1SR- 141019/899
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.			
			CVE ID : CVE-2019-16649			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-A1SR- 141019/900	
a1sri-2758f_fi	irmuaro		CVE ID : CVE-2019-16650			
alsn-2/581_1	Irmware		On Current U11 U12	 		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-A1SR- 141019/901	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-A1SR- 141019/902	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
	<i>a</i>		CVE ID : CVE-2019-16650				
a1srm-2558f_	Irmware		On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.			0-SUP-/ 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-7 141019	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & C	/E ID	Patch	NCIIP	C ID
			CVE ID : CVE-2019	·16650			
a1srm-2758f_	firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11 M11, X9, X10, and X products, a combinate encryption and authentication probethe virtual media se allows capture of BN credentials and data transferred over vir media devices. Attact use captured creder connect virtual USB to the server manage BMC.	11 ation of lems in rvice MC tual ckers can atials to devices ed by the	/A	O-SUP-A 141019,	
Improper Privilege Management a1srm-ln5f-2 :	20-09-2019 358 firmware	7.5	CVE ID : CVE-2019 On Supermicro X10 products, a client's a privileges may be transferred to a diffe client that later has socket file descripto number. In opportu circumstances, an at can simply connect virtual media service then connect virtual devices to the serve managed by the BM CVE ID : CVE-2019	and X11 access erent the same r nistic tacker to the e, and l USB r C.	/A	O-SUP-A 141019,	
a15111-11151-2.	550_III IIIwai e	-	0 0 1 144	114.0			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC		/A	0-SUP-A 141019,	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5	5-6 6	5-7 7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-A1SR- 141019/908
a1srm-ln7f-2	358_firmware	9			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-A1SR- 141019/909
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-A1SR-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	PC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	/910
a1srm-ln7f-2	758_firmware	9					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-4 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		0-SUP-/ 141019	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	C ID
				es to the ged by t						
				D : CVE-						
b10drc-n_firm	nwaro		CVEI	DICVE	2019-1	.0030				
DIVUIC-II_IIII	liwale		On Su		o II11 I	112	[
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.				N/A		0-SUP-I 141019	
			CVE I	D : CVE-	2019-1	.6649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		N/A		0-SUP-I 141019			
b10drc_firmv	b10drc_firmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		0-SUP-I 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-I 141019	
x10drff-ctg_fit	rmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-1664	9	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X products, a client's access privileges may be transferred to a different client that later has the sa socket file descriptor number. In opportunistic circumstances, an attacke can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-1665	ime Pr N/A	O-SUP-X10D- 141019/918
x10drff-ig_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers use captured credentials connect virtual USB device to the server managed by BMC. CVE ID : CVE-2019-1664	of in N/A can to res the	O-SUP-X10D- 141019/919
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X products, a client's access privileges may be transferred to a different client that later has the sa socket file descriptor number. In opportunistic circumstances, an attacke	me N/A	O-SUP-X10D- 141019/920
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5 315	-6 6-7	7-8 8-9 9-10

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				215						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.					
			CVE ID : CVE-2019-16650					
x10drff-itg_fir	mware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/921			
			CVE ID : CVE-2019-16649					
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/922			
x10drff_firmware								
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10			

Credentials Improper Privilege Management P.5 Products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. Improper Privilege Privileg	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management20-09-20197.5products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic cra simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.N/A0-SUP-X10D- 141019/924Store in the server managed by the BMC.ON Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentialsN/A0-SUP-X10D- 141019/924Use of Hard- coded Credentials0.013.44.55.66.77.88.90.10	Credentials			encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		141019/923
Use of Hard- coded Credentials 20-09-2019 5 Credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices 20-00-00-00-00-00-00-00-00-00-00-00-00-0	Privilege	20-09-2019	7.5	products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	
Use of Hard- coded Credentials $20-09-2019 $ $5 $ $5 $ $5 $ $1 + Virtual media serviceallows capture of BMCcredentials and datatransferred over virtualmedia devices. Attackers canuse captured credentials toconnect virtual USB devices 4 $	x10drfr-n_firi	mware				
	coded	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to	N/A	
	CV Scoring Scale (CVSS)	e 0-1	1-2		6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/926
			CVE ID : CVE-2019-16650		
x10drfr-nt_fin	rmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/927
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D- 141019/928
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	'C ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10drfr-t_firn	nware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by to BMC. CVE ID : CVE-2019-16649	n N/A an o s he		O-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X1 products, a client's access privileges may be transferred to a different client that later has the san socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	ne N/A		O-SUP-X 141019	
x10drfr_firmware							
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-X10D- 141019/931
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/932
x10drg-h_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10D- 141019/933
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/934
x10drg-ht_fir	mware		CVE ID : CVE-2019-16650		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/935
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10D- 141019/936
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
x10drg-o+-cp	u firmuara		CVE ID : CVE-2019-16650				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16650					
x10drg-ot+-cpu_firmware								
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/939			
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/940			
x10drg-q_firm	nware			L				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10D- 141019/941			
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/942
x10drh-c_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/943
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIP	CID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		141019,	/944
x10drh-cln4_	firmware					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-X 141019,	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A	0-SUP-X 141019,	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
				es to the ged by t						
				D : CVE-						
x10drh-ct_fir	mwaro		CVEI	DICVE	2019-1	.0030				
	lliwale		0		. 1111 1	110	[[
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede trans media use ca conne	apermicr X9, X10, acts, a co ption an intication rtual me s captur ntials ar ferred ov a devices aptured ect virtua	and X1 ombination of problection of BM of data over virtue s. Attack credent al USB d	1 ion of ems in vice C nal ters can ials to evices	N/A		O-SUP-X 141019	-
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	produ privil trans client socke numb circun can si virtua then o devic mana	ipermicr icts, a cli eges may ferred to t file des t file des oer. In op mstances mply co al media connect es to the ged by t D : CVE -	ient's ac y be o a differ er has th scriptor portunt s, an atta nnect to service, virtual U server he BMC.	cess rent ne same istic acker o the and JSB	N/A		0-SUP-X 141019	
x10drh-i_firm	iware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in		N/A		0-SUP-X 141019			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	h	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			0-SUP-> 141019	
x10drh-iln4_f	îrmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers car use captured credentials to connect virtual USB devices to the server managed by the BMC.			0-SUP-> 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

2	2	7
- 3	Z	/
_		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-16649							
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/952					
			CVE ID : CVE-2019-16650							
x10drh-it_firmware										
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/953					
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D- 141019/954					
CV Scoring Scal	0		22 24 45 56							

(CVSS)				270						
CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		
x10dri-ln4+_f	irmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/955
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/956
x10dri-t4+_fi	rmware				
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 329	6-7 7-	8 8-9 9-10

Credentials							
			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	9/957
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-2 141019	
x10dri-t_firmw	vare						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-2 141019	
CV Scoring Scale	0-1	1-2	2-3 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 the server managed by the BMC.						
			CVE ID : CVE-2019-16649						
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/960				
			CVE ID : CVE-2019-16650						
x10dri_firmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/961				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D- 141019/962				
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	'C ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
x10drl-c_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649	N/A n n		0-SUP-} 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X1 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	ne N/A		O-SUP-} 141019	
x10drl-ct_firm	nware						
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-X10D- 141019/965
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/966
x10drl-i_firm	ware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A	O-SUP-X10D- 141019/967
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/968
x10drl-it_firm	wara		CVE ID : CVE-2019-16650		
	Iware		On Supermicro H11, H12,		
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/969
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10D- 141019/970
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	C ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16650				
x10drl-ln4_fir	mwale		On Supermicro H11, H12,				
Use of Hard- coded Credentials	20-09-2019	5	M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16650		
x10drs_firmw	vare				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/973
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/974
x10drt-b+_fir	mware			I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X10D- 141019/975
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/976
x10drt-h_firm	iware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/977
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	/978
x10drt-hibf_fi	irmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			0-SUP-X 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		0-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
				es to the ged by tl						
				D : CVE -						
v10dat firm			CVEI	D.CVE-	2019-1	0030				
x10drt-l_firm	ware		0.6			110	[
Use of Hard- coded Credentials	20-09-2019	5	M11, 2 produ encry authe the vir allows credes transf media use ca conne	permicr X9, X10, acts, a co ption an ntication rtual me s captur ntials an ferred ov a devices aptured ov ect virtua server n	and X1 mbinati d n proble edia serv e of BM d data ver virtu s. Attack credent al USB d	1 ion of ems in vice C ual ters can ials to	N/A		O-SUP-X 141019	-
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	produ privile transf client socke numb circur can si virtua then c device manag	permicr acts, a cli eges may erred to that late t file des er. In op nstances mply co al media connect es to the ged by th D : CVE-	ent's ac y be a differ er has th criptor portuni s, an atta nnect to service, virtual U server he BMC.	cess rent ne same istic acker o the and JSB	N/A		O-SUP-X 141019	
x10drt-libf_fi	rmware									
Use of Hard- coded Credentials	20-09-2019	5	M11, 2 produ encry	permicr X9, X10, Icts, a co ption an ntication	and X1 mbinati d	1 ion of	N/A		0-SUP-X 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pat	ch	NCIIP	C ID
			the virtual m allows captur credentials a transferred o media device use captured connect virtu to the server BMC. CVE ID : CVE	re of BM(nd data over virtu s. Attack credenti al USB d manageo	al ers can als to evices l by the				
Improper Privilege Management	20-09-2019	7.5	On Supermic products, a cl privileges ma transferred t client that lat socket file de number. In o circumstance can simply co virtual media then connect devices to the managed by t	lient's act ay be o a differ cer has th scriptor pportuni es, an atta onnect to a service, virtual U e server the BMC.	cess ent e same stic acker the and JSB	N/A		0-SUP-2 141019	
x10drt-libq_fi	rmware								
Use of Hard- coded Credentials	20-09-2019	5	On Supermic M11, X9, X10 products, a co encryption and authentication the virtual m allows capture credentials and transferred of media device use captured connect virtuant to the server BMC.	, and X11 ombinati nd on proble edia serv re of BM0 nd data over virtu s. Attack credenti al USB d	l on of ms in rice C al ers can als to evices	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/986
			CVE ID : CVE-2019-16650		
x10drw-e_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/987
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-X10D- 141019/988
CV Scoring Scale	e 0-1		2-3 3-4 4-5 5-6	6-7 7-8	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				341						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		
x10drw-et_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/989
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/990
x10drw-n_firm	mware			T	
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A	O-SUP-X10D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 342	6-7 7-8	8 8-9 9-10

		CVSS	Description & CVE ID	Pat	CII	NCIIF	PC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	9/991
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-2 141019	
x10drx_firmwa	are						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-2 141019	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/994
			CVE ID : CVE-2019-16650		
x10dsn-ts_firm	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/995
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D- 141019/996
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		
x10obi-cpu_fi	rmware			·	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		O-SUP-X100- 141019/997
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X100- 141019/998
x10qbi_firmw	vare				
	e o i				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X10Q- 141019/999
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X10Q- 141019/1000
x9drd-ef_firm	iware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca	N/A	O-SUP-X9DR- 141019/1001
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			use captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
x9drd-it+_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1002
x9drd-l/if_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1003
x9drff(-7)_fir	mware			1	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
				2/17						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1004
x9drff-7/i(t)+	firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1005
x9drff-7/i(t)g	+_firmware			I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X9DR- 141019/1006
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
x9drfr_firmwa	are				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1007
x9drg-h(t)f+_	firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		O-SUP-X9DR- 141019/1008
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID				Pat	tch	NCIIP	C ID
			CVE I	D : CVE-	2019-1	6649				
x9drg-h(t)f+i	i_firmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			N/A		0-SUP-7 141019		
x9drg-h(t)f_fi	rmware		UTEI		-0171	0017				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		N/A		0-SUP-X 141019			
x9drg-o(t)f-cp	pu_firmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		0-SUP-X 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descriptio	Pat	ch	NCIIP	PC ID		
			the virtual me allows captur credentials ar transferred ov media devices use captured connect virtua to the server of BMC.						
x9drg-qf_firm	ware					I		1	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		N/A		O-SUP-2 141019		
x9drh-7/i(t)f	firmware								
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices			N/A		O-SUP-2 141019	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE	ID	Patc	h	NCIIP	C ID
			to the server manage BMC.	d by the				
			CVE ID : CVE-2019-1	6649				
x9drh-if-nv_fi	rmware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and dataItransferred over virtual media devices. Attackers can use captured credentials to 		N/A		O-SUP-≯ 141019	
x9drl-3/if_fir	mware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		N/A		O-SUP-X 141019	
x9drl-7/ef_fir	mwaro		CVE ID : CVE-2019-1					
	mwale		0.0.1	112			O-SUP->	קטע
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11		N/A		141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 352	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
x9drt-h_serie	s_firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1017
x9drt-hf+_firm	nware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual	N/A	O-SUP-X9DR- 141019/1018
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
x9drt-p_serie	s_firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1019
x9drt_series_t	firmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1020

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				25/						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
x9drw-3/if_fi	rmware	1			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	0-SUP-X9DR- 141019/1021
x9drw-3ln4f+	-/3tf+_firmwa	re			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9DR- 141019/1022
x9drw-7/itpf	+_firmware			·	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service	N/A	0-SUP-X9DR- 141019/1023
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
x9drw-7/itpf_	firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
x9drw-c(t)f31	_firmware			I			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patc	h	NCIIP	C ID
			BMC.				
			CVE ID : CVE-2019-16649				
x9drx+-f_firm	ware			·			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC.	N/A n		O-SUP-X9DR- 141019/1026	
			CVE ID : CVE-2019-16649				
x9qr7-tf+_firm	nware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649	ne		0-SUP-X 141019	•
x9qr7-tf_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of	N/A		0-SUP-X 141019	-
CV Scoring Scale			2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIPO	DID	
			encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.					
			CVE ID : CVE-2019-16649					
x9qri-f+_firm	ware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-X 141019/	-	
x9qri-f_firmw	are							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can	N/A		O-SUP-X 141019/	-	
CV Scoring Scale (CVSS)	CV Scoring Scale (CVSS) 0-1 1-2 2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
x9sae(-v)_firm	nware			<u> </u>	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A	0-SUP-X9SA- 141019/1031
			CVE ID : CVE-2019-16649		
x9sca(-f)_firm	iware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X9SC- 141019/1032
x9scd_series_	firmware		GVE ID : GVE-2017-10049		
CV Scoring Scal	e				

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				359						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		0-SUP-X9SC- 141019/1033	
x9sci-ln4(f)_fi	irmware					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X9SC- 141019/1034	
x9scl(-f)_firm	ware			I		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A	O-SUP-X9SC- 141019/1035	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	CID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16649				
x9scl+-f_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
x9scm(-f)_firm	nware			I		I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 361	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
			CVE I	D : CVE·	2019-1	.6649				
x9sra_firmwa	re									
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede trans media use ca conne to the BMC.		and X1 ombinat d n proble edia serv e of BM d data ver virtu s. Attack credent al USB d manage	1 ion of ems in vice C ual ters can ials to evices d by the	N/A		O-SUP-2 141019	
			CVE I	D : CVE-	2019-1	.6649				
x9srd-f_firmw	vare									
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede trans media use ca conne to the BMC.	permicr X9, X10, acts, a co ption an entication rtual me s captur ntials ar ferred or a devices aptured ect virtua e server a D : CVE -	and X1 ombinat od n proble edia serv e of BM od data ver virtu s. Attack credent al USB d manage	1 ion of ems in vice C all ters can ials to evices d by the	N/A		O-SUP-2 141019	
x9sre/i_serie	s_firmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in		X11 O-SUP- nation of N/A 141019		0-SUP-2 141019			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
			the virtual me allows captur credentials an transferred ov media devices use captured connect virtua to the server of BMC.	e of BMC nd data ver virtu s. Attacko credenti al USB do managec	al ers can als to evices l by the				
x9srg-f_firmw	vare					I		1	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicr M11, X9, X10, products, a co encryption an authentication the virtual me allows captur credentials an transferred ov media devices use captured connect virtua to the server n BMC.	and X11 ombination d n proble edia serv e of BMC d data ver virtu s. Attacko credenti al USB do managec	on of ms in ice al ers can als to evices l by the	N/A		O-SUP-2 141019	
x9srh-7(t)f_fi	rmware					<u> </u>		I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices		N/A		O-SUP-2 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description	n & CVE ID	Pat	ch	NCIIP	CID
			to the server m BMC.	anaged by the				
			CVE ID : CVE-2	019-16649				
x9srl(-f)_firm	ware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro M11, X9, X10, a products, a con encryption and authentication the virtual med allows capture credentials and transferred ove media devices. use captured cr connect virtual to the server m BMC. CVE ID : CVE-2	and X11 abination of problems in lia service of BMC l data er virtual Attackers can redentials to USB devices anaged by the	N/A		0-SUP-X 141019	
x9srw-f_firm	ware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro M11, X9, X10, a products, a com encryption and authentication the virtual med allows capture credentials and transferred ove media devices. use captured cr connect virtual to the server m BMC. CVE ID : CVE-2	and X11 abination of problems in lia service of BMC l data er virtual Attackers can redentials to USB devices anaged by the	N/A		0-SUP-X 141019	
b10drg-ibf2_f	firmware							
Use of Hard- coded	20-09-2019	5	On Supermicro M11, X9, X10, a		N/A		0-SUP-I 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 364	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	e N/A		O-SUP-1 141019	
b10drg-ibf_fi	rmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		0-SUP-1 141019	
CV Scoring Scal	e 0-1	1-2	2-3 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 the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-B10D- 141019/1048
			CVE ID : CVE-2019-16650		
b10drg-tp_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-B10D- 141019/1049
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-B10D- 141019/1050
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	:h	NCIIPO	D
			number. In opportunistic circumstances, an attack can simply connect to the virtual media service, an then connect virtual USE devices to the server managed by the BMC. CVE ID : CVE-2019-166	ter e ld 3			
b10dri-n_firm	iware			· · ·			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12 M11, X9, X10, and X11 products, a combination encryption and authentication problems the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers use captured credentials connect virtual USB devi to the server managed by BMC. CVE ID : CVE-2019-166	of s in e N/A s can s to ices y the		-SUP-B 1019/	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and products, a client's access privileges may be transferred to a different client that later has the s socket file descriptor number. In opportunistic circumstances, an attack can simply connect to th virtual media service, an then connect virtual USE devices to the server managed by the BMC. CVE ID : CVE-2019-166	ss t same c ter e id 3		-SUP-B 1019/	
b10dri_firmw	are						
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-B10D- 141019/1053
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-B10D- 141019/1054
b10drt-ibf2_f	irmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers cap	N/A	O-SUP-B10D- 141019/1055
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description a	& CVE ID	Pat	ch	NCIIF	°C ID
			use captured cre connect virtual U to the server ma BMC.	JSB devices				
			CVE ID : CVE-20	19-16649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X products, a clien privileges may b transferred to a client that later h socket file descri number. In oppo circumstances, a can simply conne virtual media sen then connect vir devices to the se managed by the CVE ID : CVE-20	t's access e different has the same ptor rtunistic n attacker ect to the rvice, and tual USB rver BMC.	N/A		0-SUP- 141019	
b10drt-ibf_fir	mware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H M11, X9, X10, an products, a comb encryption and authentication p the virtual media allows capture of credentials and of transferred over media devices. A use captured cree connect virtual U to the server ma BMC. CVE ID : CVE-20	d X11 pination of roblems in a service f BMC data virtual ttackers can dentials to JSB devices naged by the	N/A		O-SUP- 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different		N/A		0-SUP- 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
b10drt-tp_firr	nware		CAE ID . CAE-2013-10030				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-F 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP-F 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	Patch		CID
			CVE ID : CVE-2019-16650				
b10drt_firmw	are					I	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-E 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-E 141019	
b11dpe_firmv	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A		O-SUP-E 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-B11D- 141019/1064
b11dpt_firmw	vare				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-B11D- 141019/1065
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-B11D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	[Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650						141019	/1066
b11qpi_firmw	vare									
Use of Hard- coded Credentials	20-09-2019	5	M11, 2 produ encry authe the vir allows credes transf media use ca conne to the BMC.	permicr X9, X10, acts, a co ption an ntication rtual me s captur ntials an ferred ov a devices ptured ov ect virtua server n D : CVE-	and X1 ombination of problection of BM of data ver virtue s. Attack credent al USB d manage	1 ion of ems in vice C al ters can ials to evices d by the	N/A		O-SUP-I 141019	•
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB		N/A		O-SUP-I 141019	-		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	ch	NCIIP	CID
				es to the ged by t						
				$\mathbf{D}: \mathbf{CVE}$						
b11spe-cpu-2	5g firmwara		CVEI	DICVE	2019-1	0030				
D11Spe-cpu-2	.5g_III III wai e		On Su			110	[[
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede trans media use ca conne	apermicr X9, X10, acts, a co ption an entication rtual me s captur ntials ar ferred or a devices aptured ect virtus	and X1 ombinati d n proble edia serv e of BM nd data ver virtu s. Attack credent al USB d	1 ion of ems in vice C nal ters can ials to evices	N/A		O-SUP-I 141019	
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		N/A		0-SUP-I 141019			
b11spe-cpu-t	f_firmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		0-SUP-I 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description 8	& CVE ID	Pat	ch	NCIIP	'C ID
			the virtual media allows capture of credentials and d transferred over media devices. At use captured cree connect virtual U to the server man BMC. CVE ID : CVE-20					
Improper Privilege Management	20-09-2019	7.5	On Supermicro X products, a client privileges may be transferred to a c client that later h socket file descrip number. In oppor circumstances, an can simply connec virtual media ser then connect virt devices to the ser managed by the h	c's access e different as the same ptor rtunistic n attacker ect to the rvice, and cual USB cver BMC.	N/A		O-SUP-1 141019	
b1sd1-16c-tf_	firmware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		N/A		O-SUP-1 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4	l-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-B1SD- 141019/1074
			CVE ID : CVE-2019-16650		
b1sd1-tf_firm	ware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-B1SD- 141019/1075
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	O-SUP-B1SD- 141019/1076
CV Scoring Scale	e 0-1		2-3 3-4 4-5 5-6	6-7 7-8	

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

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	h	NCIIP	C ID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
b1sd2-16c-tf_	firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-E 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-E 141019	
b1sd2-tf_firm	ware						
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-E	B1SD-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 377	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	:h	NCIIF	PC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			141019	9/1079
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP- 141019	
b2ss1-cf_firm	ware			1			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		O-SUP-1 141019	
	•						-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-B2SS- 141019/1082
			CVE ID : CVE-2019-16650		
b2ss1-cpu_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-B2SS- 141019/1083
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	0-SUP-B2SS- 141019/1084
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		
b2ss1-f_firmw	vare				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-B2SS- 141019/1085
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-B2SS- 141019/1086
b2ss1-h-mtf_f	irmware				
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8 8-9 9-10

Weakness	Publish Date	CVSS	Descrip	tion & CVE	ID	Pat	ch:	NCIIP	CID
Use of Hard- coded Credentials	20-09-2019	5	On Supermi M11, X9, X1 products, a encryption a authenticati the virtual m allows captured credentials a transferred media device use captured connect virt to the serve BMC. CVE ID : CV	0, and X1 combinat and on proble nedia serv ure of BM and data over virtu es. Attack d credent cual USB d r manage	1 ion of ems in vice C al ters can ials to evices d by the	N/A		O-SUP-I 141019	
Improper Privilege Management	20-09-2019	7.5	CVE ID : CVE-2019-16649 On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			N/A		0-SUP-I 141019	
b2ss1-mtf_fir	mware								
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can			N/A		0-SUP-I 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-B2SS- 141019/1090
b2ss2-f_firmw	vare				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-B2SS- 141019/1091
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	0-SUP-B2SS- 141019/1092
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	tch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
b2ss2-h-mtf_f	firmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			O-SUP-1 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-1 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID		Pat	ch	NCIIP	CID
			CVE ID : CVE-	-2019-16650				
b2ss2-mtf_fir	mware				1			
Use of Hard- coded Credentials	20-09-2019	5	the virtual me allows captur credentials ar transferred ov media devices use captured connect virtua to the server of BMC.	and X11 ombination of ad n problems in edia service re of BMC ad data ver virtual s. Attackers can credentials to al USB devices managed by the	N/A		O-SUP-I 141019	
Improper Privilege Management	20-09-2019 are	7.5	On Supermicr products, a cli privileges may transferred to client that late socket file des number. In op circumstances can simply co virtual media then connect devices to the managed by t	y be a different er has the same scriptor oportunistic s, an attacker nnect to the service, and virtual USB e server	N/A		O-SUP-I 141019	
b)ui/_iiiiiwa								
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC		N/A		O-SUP-I 141019	
CV Scoring Scal	e 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pato	ch	NCIII	PCID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16649				
b9drg-3m_fir	mware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP- 141019	
b9drg-e_firm	ware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.	N/A		0-SUP- 141019	
CV Scoring Scale							

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	ch	NCIIP	CID	
			CVE ID : CVE-2019-16649							
b9drg_firmwa	are		I				<u> </u>		I	
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede transt media use ca conne to the BMC.	permicr X9, X10, acts, a co ption an entication rtual me s captur ntials an ferred ov a devices aptured o ect virtua e server n D : CVE-	and X12 mbinati d n proble dia serv e of BM0 d data ver virtu s. Attack credenti al USB d manageo	1 on of ems in vice C nal ters can tials to evices d by the	N/A		0-SUP-I 141019	
b9dri_firmwa	Ire		CVEI	D:CVE-	2019-1	0049				
b)ull_iniwa			On Su	ipermicr	o U11 I	J17			[
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede transt media use ca conne to the BMC.	X9, X10, acts, a co ption an entication rtual me s capture ntials an ferred ov a devices aptured o ect virtua e server n D : CVE-	and X12 mbinati d n proble edia serv e of BM0 d data ver virtu s. Attack credenti al USB d manageo	1 con of ems in vice C nal ers can ials to evices d by the	N/A		0-SUP-H 141019	
b9drp_firmwa	are						I			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in		N/A		O-SUP-I 141019			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649				
b9drt_firmwa	ire		I			l	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-I 141019	
b9qr7(-tp)_fir	rmware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices	N/A		0-SUP-I 141019	-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description	& CVE ID	Pat	ch	NCIIP	CID
			to the server ma BMC.	anaged by the				
			CVE ID : CVE-2	019-16649				
m11sdv-4c-ln	4f firmware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		N/A		O-SUP-N 141019	
m11sdv-4ct-l	n4f_firmware							
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		N/A		O-SUP-N 141019	
m11cdy 9a	hAf firmward		CVE ID : CVE-20	017 10047				
m11sdv-8c+-		-	0.0				O-SUP-N	M11C
Use of Hard- coded	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11		N/A		0-SOP-1 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 388	4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Description	on & CVE	ID	Pat	tch	NCIIP	C ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649							
m11sdv-8c-ln	4f_firmware									
Use of Hard- coded Credentials	20-09-2019	5	M11, produ encry authe the vi allow crede trans media use ca conne to the BMC.	permicr X9, X10, acts, a co ption ar enticatio rtual me s captur entials ar ferred or a devices aptured ect virtu e server r D : CVE	and X1 ombinati nd n proble edia serv e of BM0 nd data ver virtu s. Attack credenti al USB d manageo	1 on of ems in vice C al ers can ials to evices d by the	N/A		O-SUP-1 141019	
m11sdv-8ct-l	n4f_firmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual			N/A		O-SUP-N 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	PC ID
			media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.				
			CVE ID : CVE-2019-16649				
x10dbt-t_firm	iware						
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		0-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		0-SUP-2 141019	-
x10ddw-i_firm	nware						
Use of Hard-	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11	N/A		O-SUP-2	X10D-
coded			, , , -,				

Weakness	Publish Date	CVSS	Dese	cription	& CVE	ID	Pat	tch	NCIIP	PC ID
Credentials			products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649						141019)/1112
Improper Privilege Management	20-09-2019	7.5	On Super products privilege transferr client tha socket fil number. circumsta can simp virtual m then com devices to managed CVE ID :	, a clien s may b red to a at later l e descr In oppo ances, a ly conn redia se nect vir o the se l by the	t's actored differ has the iptor ortuni an atta ect to rvice, tual U erver BMC.	cess ent e same stic acker the and JSB	N/A		O-SUP-2 141019	
x10ddw-in_fi	rmware								<u> </u>	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices			N/A		0-SUP-2 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3	8-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/1115
			CVE ID : CVE-2019-16650		
x10dgo-t_firm	iware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/1116
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor	N/A	O-SUP-X10D- 141019/1117
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC	ID
			number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			
x10dgq_firmv	vare					
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X1 141019/3	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X1 141019/1	
x10drc-ln4+_i	firmware					
CV Scoring Scale	e 0-1	1-2	2-3 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 of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca use captured credentials to connect virtual USB devices to the server managed by th BMC. CVE ID : CVE-2019-16649		O-SUP-X10D- 141019/1120
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X12 products, a client's access privileges may be transferred to a different client that later has the sam socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		O-SUP-X10D- 141019/1121
x10drc-t4+_fi	rmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers ca	N/A	O-SUP-X10D- 141019/1122
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 captured credentials to connect virtual USB devices to the server managed by the BMC.		
			CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/1123
x10drd-i_firm	ware		CVE ID : CVE-2019-16650		
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/1124
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different	N/A	O-SUP-X10D- 141019/1125
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.				
x10drd-int_fi			CVE ID : CVE-2019-16650				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A		O-SUP-X10D- 141019/1127	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch		NCIIPC IE)
			CVE ID : CVE-2019-16650				
x10drd-intp_f	firmware			I			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A		O-SUP-X10 141019/12	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A		O-SUP-X10 141019/12	
x10drd-it_firm	nware			I			
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC	N/A		O-SUP-X10 141019/12	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6 397	6-7 7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650	N/A	O-SUP-X10D- 141019/1131
x10drd-itp_fi	rmware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/1132
Improper	20-09-2019	7.5	On Supermicro X10 and X11	N/A	O-SUP-X10D-
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	:ch	NCIIF	PC ID
Privilege Management			products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650			141019	9/1133
x10drd-l_firm	iware					<u> </u>	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649			O-SUP-2 141019	
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB	N/A		O-SUP-2 141019	
CV Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descriptio	on & CVE	ID	Pat	tch	NCIIP	CID
				es to the ged by t						
				$\mathbf{D}: \mathbf{CVE}$						
x10drd-lt_firm	nwara		CVEI	DICVE	2019-1	0030				
x10u1u-1t_1111	liwale		0	permicr	. 1111 1	110	[[
Use of Hard- coded Credentials	20-09-2019	5	products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.		encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the		O-SUP-X 141019	-		
			CVE I	D : CVE-	2019-1	6649				
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650		N/A		0-SUP-X 141019			
x10drd-ltp_fin	rmware									
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in			N/A		0-SUP-X 141019		
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	C	Descriptio	on & CVE	ID	Pat	tch	NCIIF	PC ID
			the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649							
Improper Privilege Management	20-09-2019	7.5	produ privile transfe client socket numbe circun can sin virtua then c device manag	permicr cts, a cli eges may erred to that late t file des er. In op nstances mply co l media onnect es to the ged by t	ient's ac y be o a differ er has th scriptor portun s, an att nnect to service virtual l server he BMC	rent ne same istic acker o the , and JSB	N/A		0-SUP-2 141019	
x10drff-c_firm	nware								<u> </u>	
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC.				N/A		0-SUP-2 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3	3-4 401	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-2019-16649		
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC.	N/A	O-SUP-X10D- 141019/1141
			CVE ID : CVE-2019-16650		
x10drff-cg_fir	mware				
Use of Hard- coded Credentials	20-09-2019	5	On Supermicro H11, H12, M11, X9, X10, and X11 products, a combination of encryption and authentication problems in the virtual media service allows capture of BMC credentials and data transferred over virtual media devices. Attackers can use captured credentials to connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16649	N/A	O-SUP-X10D- 141019/1142
Improper Privilege Management	20-09-2019	7.5	On Supermicro X10 and X11 products, a client's access privileges may be transferred to a different client that later has the same socket file descriptor number. In opportunistic circumstances, an attacker	N/A	0-SUP-X10D- 141019/1143
CV Scoring Scale	e 0-1		2-3 3-4 4-5 5-6	6.7 7.	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				402						

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			can simply connect to the virtual media service, and then connect virtual USB devices to the server managed by the BMC. CVE ID : CVE-2019-16650				
telestar			CVE ID : CVE-2019-10050				
imperial_i450) firmware						
			TELESTAR Bobs Rock Radio,				
Improper Authenticati on	16-09-2019	7.5	Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. CVE ID : CVE-2019-13474	N/A		O-TEL-1 141019	
imperial_i500)-bt_firmware	:					
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml,	N/A		O-TEL-1 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	C ID
			/Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands.				
haha waala wa	die <i>G</i> immene		CVE ID : CVE-2019-13474				
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200 Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. CVE ID : CVE-2019-13474),		O-TEL-1 141019	
dabman_d10_	firmware						
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200 Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol,),		O-TEL-1 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pate	ch	NCIIP	C ID
			/hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands.				
			CVE ID : CVE-2019-13474				
dabman_i30_s	stereo_firmwa	are					
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radi Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i20 Imperial i200-cd, Imperial i400, Imperial i450, Imperi i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. CVE ID : CVE-2019-13474	0, al N/A		O-TEL-I 141019	
imperial_i110)_firmware						
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radi Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i20 Imperial i200-cd, Imperial i400, Imperial i450, Imperi i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init,	0,		O-TEL-I 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			/playlogo.jpg, /stop, /exit, /back, and /playinfo commands.				
			CVE ID : CVE-2019-13474				
imperial_i150	_firmware			1			
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. CVE ID : CVE-2019-13474	N/A		O-TEL-I 141019	
imperial_i200)-cd_firmware	;					
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit,	N/A		O-TEL-I 141019	
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Pat	ch	NCIIP	CID
			/back, and /playinfo commands.				
			CVE ID : CVE-2019-13474				
imperial_i20()_firmware						
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands.	N/A		O-TEL-I 141019	
			CVE ID : CVE-2019-13474				
imperial_i400)_firmware			Γ			
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo	N/A		O-TEL-I 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	D	escriptio	on & CVE	ID	Pat	ch	NCIIP	C ID
			commands.							
			CVE ID	: CVE-	2019-1	3474				
imperial_i600)_firmware									
Improper Authenticati on	16-09-2019	7.5	TELESTAR Bobs Rock Radio, Dabman D10, Dabman i30 Stereo, Imperial i110, Imperial i150, Imperial i200, Imperial i200-cd, Imperial i400, Imperial i450, Imperial i500-bt, and Imperial i600 TN81HH96-g102h-g102 devices have insufficient access control for the /set_dname, /mylogo, /LocalPlay, /irdevice.xml, /Sendkey, /setvol, /hotkeylist, /init, /playlogo.jpg, /stop, /exit, /back, and /playinfo commands. CVE ID : CVE-2019-13474		n i30 al i200, verial nperial i600 .02 ent , xml, /exit,		O-TEL-I 141019			
Tendacn	<u> </u>		<u> </u>				<u> </u>			
n301_firmwa	re									
Improper Input Validation	19-09-2019	7.8	In goform/setSysTools on Tenda N301 wireless routers, attackers can trigger a device crash via a zero wanMTU value. (Prohibition of this zero value is only enforced within the GUI.) CVE ID : CVE-2019-16412			N/A		O-TEN- 141019		
topcon	I						I		I	
net-g5_firmw	are									
Improper Privilege Management	20-09-2019	6.5	An issue was discovered on Topcon Positioning Net-G5 GNSS Receiver devices with firmware 5.2.2. The web interface of the product is				N/A		O-TOP- 141019	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS		Descripti	on & CVE	ID	Pat	tch	NCIIF	PC ID
			is allo logge attach to rea admin same regul admin The g the de	owed to d in as a ker can l nd the pa nistrativ procedu ar user t nistrativ uest log efault co	a login. A login. On guest, a prowse a prowse a assword re user. T ure allow to gain re privile in is pos pnfigurat - 2019-1	nce in a URL of the The vs a eges. ssible in cion.				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-09-2019	4	An issue was discovered on Topcon Positioning Net-G5 GNSS Receiver devices with firmware 5.2.2. The web interface of the product has a local file inclusion vulnerability. An attacker with administrative privileges can craft a special URL to read arbitrary files from the device's files system. CVE ID : CVE-2019-11327				N/A		0-TOP- 141019	
Tridium	<u> </u>								<u> </u>	
niagara4										
Improper Authenticati on	24-09-2019	2.1	A specific utility may allow an attacker to gain read access to privileged files in the Niagara AX 3.8u4 (JACE 3e, JACE 6e, JACE 7, JACE- 8000), Niagara 4.4u3 (JACE 3e, JACE 6e, JACE 7, JACE- 8000), and Niagara 4.7u1 (JACE-8000, Edge 10). CVE ID : CVE-2019-13528			N/A		0-TRI-N 141019		
niagara_ax			1				1		1	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Descript	ion & CVE	ID	Pat	ch.	NCIIP	C ID	
Improper Authenticati on	24-09-2019	2.1	A specific uti an attacker to access to priv the Niagara A 3e, JACE 6e, J 8000), Niaga 3e, JACE 6e, J 8000), and N (JACE-8000, CVE ID : CVE	o gain rea vileged fi AX 3.8u4 ACE 7, JA ra 4.4u3 ACE 7, JA iagara 4. Edge 10)	ad les in (JACE .CE- (JACE .CE- 7u1	N/A		0-TRI-NIAG 141019/115		
vandyvape				<u> </u>						
swell_kit_mod	l_firmware									
Exposure of Resource to Wrong Sphere	23-09-2019	3.3	An issue was discovered on Swell Kit Mod devices that use the Vandy Vape platform. An attacker may be able to trigger an unintended temperature in the victim's mouth and throat via Bluetooth Low Energy (BLE) packets that specify large power or voltage values. CVE ID : CVE-2019-16518			N/A		O-VAN- 141019		
Vmware			<u> </u>			<u> </u>				
esxi										
Out-of- bounds Read	20-09-2019	5.5	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650- 201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6) and Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain an out-of-bounds read vulnerability in the pixel shader functionality. Successful exploitation of this issue may lead to			https:/ w.vmv om/se y/advi s/VMS 2019- 0012.I	vare.c curit sorie A-	O-VMW 141019		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Weakness	Publish Date	CVSS	Descriptio	on & CVE	ID	Pa	tch	NCIIP	C ID
			information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on the host. Exploitation of this issue require an attacker to have access to a virtual machine with 3D graphics enabled. It is not enabled by default on ESXi and is enabled by default on Workstation and Fusion. CVE ID : CVE-2019-5521						
westerndigita	l								
wd_my_book_									
Improper Authenticati on	18-09-2019	7.5	Western Digital WD My Book World through II 1.02.12 suffers from Broken Authentication, which allows an attacker to access the /admin/ directory without credentials. An attacker can easily enable SSH from /admin/system_advanced.p hp?lang=en and login with the default root password welc0me. CVE ID : CVE-2019-16399			N/A		O-WES- WD_M- 141019	
ZTE									
zxv10_b860a	tirmware								
Improper Input Validation	23-09-2019	10	All versions up to V81511329.1008 of ZTE ZXV10 B860A products are impacted by input validation vulnerability. Due to input validation, unauthorized users can take advantage of this vulnerability to control			http://supp ort.zte.com. cn/support /news/Loo pholeInfoD etail.aspx?n ewsId=101		0-ZTE-ZXV1- 141019/1163	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 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 user terminal system.	1263	
			CVE ID : CVE-2019-3416		
			Hardware	L	L
Schneider-ele	ectric				
hmigtu_firmv	vare				
Improper Check for Unusual or Exceptional Conditions	17-09-2019	4.3	A CWE-754 ? Improper Check for Unusual or Exceptional Conditions vulnerability exists in Magelis HMI Panels (all versions of - HMIGTO, HMISTO, XBTGH, HMIGTU, HMIGTUX, HMISCU, HMISTU, XBTGT, XBTGT, HMIGXO, HMIGXU), which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel. CVE ID : CVE-2019-6833	https://ww w.schneider - electric.com /ww/en/do wnload/doc ument/SEV D-2019- 225-01	H-SCH-HMIG- 141019/1164
Vivotek					
camera			VIVOTEK ID Comore dovices		
Improper Input Validation	on 18-09-2019 7.8 allow a denial of service via crafted HTTP header.		with firmware before 0x20x allow a denial of service via a	N/A	H-VIV-CAME- 141019/1165

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