National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Aug 2020 Vol. 07 No. 15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
accuity					
firco_continuity					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	4.3	A stored Cross-site scripting (XSS) vulnerability in Firco Continuity 6.2.0.0 allows remote unauthenticated attackers to inject arbitrary web script or HTML through the username field of the login page. **CVE ID : CVE-2020-16186**	N/A	A-ACC-FIRC-200820/1
Acti					
nvr					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	04-Aug-20	5	ActiveMediaServer.exe in ACTi NVR3 Standard Server 3.0.12.42 allows remote unauthenticated attackers to trigger a buffer overflow and application termination via a malformed payload. **CVE ID : CVE-2020-15956**	N/A	A-ACT-NVR-200820/2
Advantech					
webaccess\/hmi_designer					
Out-of-bounds Write	06-Aug-20	6.8	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. Multiple heap-based buffer overflow vulnerabilities may be exploited by	N/A	A-ADV-WEBA-200820/3

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			opening specially crafted project files that may overflow the heap, which may allow remote code execution, disclosure/modification of information, or cause the application to crash. **CVE ID : CVE-2020-16207**		
Out-of-bounds Read	06-Aug-20	4.3	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. An out-of-bounds read vulnerability may be exploited by processing specially crafted project files, which may allow an attacker to read information. **CVE ID : CVE-2020-16211**	N/A	A-ADV-WEBA-200820/4
Out-of-bounds Write	06-Aug-20	6.8	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. Processing specially crafted project files lacking proper validation of user supplied data may cause the system to write outside the intended buffer area, which may allow remote code execution, disclosure/modification of information, or cause the application to crash. **CVE ID : CVE-2020-16213**	N/A	A-ADV-WEBA-200820/5
Out-of-bounds Write	06-Aug-20	6.8	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior.	N/A	A-ADV-WEBA-200820/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing specially crafted project files lacking proper validation of user supplied data may cause a stack-based buffer overflow, which may allow remote code execution, disclosure/modification of information, or cause the application to crash. **CVE ID : CVE-2020-16215**		
Double Free	06-Aug-20	6.8	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. A double free vulnerability caused by processing specially crafted project files may allow remote code execution, disclosure/modification of information, or cause the application to crash. **CVE ID : CVE-2020-16217**	N/A	A-ADV-WEBA-200820/7
Access of Resource Using Incompatible Type ('Type Confusion')	06-Aug-20	6.8	Advantech WebAccess HMI Designer, Versions 2.1.9.31 and prior. Processing specially crafted project files lacking proper validation of user supplied data may cause a type confusion condition, which may allow remote code execution, disclosure/modification of information, or cause the application to crash. **CVE ID : CVE-2020-16229**	N/A	A-ADV-WEBA-200820/8
Aerospike					
aerospike_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	05-Aug-20	10	Aerospike Community Edition 4.9.0.5 allows for unauthenticated submission and execution of user-defined functions (UDFs), written in Lua, as part of a database query. It attempts to restrict code execution by disabling os.execute() calls, but this is insufficient. Anyone with network access can use a crafted UDF to execute arbitrary OS commands on all nodes of the cluster at the permission level of the user running the Aerospike service. **CVE ID : CVE-2020-13151**	N/A	A-AER-AERO-200820/9
Amazon					
firecracker					
N/A	04-Aug-20	4.3	In Firecracker 0.20.x before 0.20.1 and 0.21.x before 0.21.2, the network stack can freeze under heavy ingress traffic. This can result in a denial of service on the microVM when it is configured with a single network interface, and an availability problem for the microVM network interface on which the issue is triggered. **CVE ID : CVE-2020-16843**	N/A	A-AMA-FIRE-200820/10
Apache					
wicket					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	11-Aug-20	5	By crafting a special URL it is possible to make Wicket deliver unprocessed HTML templates. This would allow an attacker to see possibly sensitive information inside a HTML template that is usually removed during rendering. Affected are Apache Wicket versions 7.16.0, 8.8.0 and 9.0.0-M5 **CVE ID : CVE-2020-11976**	N/A	A-APA-WICK-200820/11
skywalking					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	05-Aug-20	7.5	**Resolved** Only when using H2/MySQL/TiDB as Apache SkyWalking storage, there is a SQL injection vulnerability in the wildcard query cases. **CVE ID : CVE-2020-13921**	N/A	A-APA-SKYW-200820/12
http_server					
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	07-Aug-20	5	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers. **CVE ID : CVE-2020-9490**	https://security.netapp.com/advisory/ntap-20200814-0005/	A-APA-HTTP-200820/13

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-20	7.5	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE **CVE ID : CVE-2020-11984**	https://security.netapp.com/advisory/ntap-20200814-0005/	A-APA-HTTP-200820/14
Insufficient Verification of Data Authenticity	07-Aug-20	4.3	IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020. **CVE ID : CVE-2020-11985**	N/A	A-APA-HTTP-200820/15
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')	07-Aug-20	4.3	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers. **CVE ID : CVE-2020-11993**	https://security.netapp.com/advisory/ntap-20200814-0005/	A-APA-HTTP-200820/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Artifex					
ghostscript					
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in lprn_is_black() in contrib/lips4/gdevlprn.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16287**	N/A	A-ART-GHOS-200820/17
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Aug-20	4.3	A buffer overflow vulnerability in pj_common_print_page() in devices/gdevpjet.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16288**	N/A	A-ART-GHOS-200820/18
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in cif_print_page() in devices/gdevcif.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16289**	N/A	A-ART-GHOS-200820/19
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in jetp3852_print_page() in devices/gdev3852.c of Artifex Software	N/A	A-ART-GHOS-200820/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16290**		
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in contrib/gdevdj9.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16291**	N/A	A-ART-GHOS-200820/21
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in mj_raster_cmd() in contrib/japanese/gdevmjc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16292**	N/A	A-ART-GHOS-200820/22
NULL Pointer Dereference	13-Aug-20	4.3	A null pointer dereference vulnerability in compose_group_nonknockout_nonblend_isolated_allmask_common() in base/gxblend.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16293**	N/A	A-ART-GHOS-200820/23

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Aug-20	4.3	A buffer overflow vulnerability in epsc_print_page() in devices/gdevepsc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16294**	N/A	A-ART-GHOS-200820/24
NULL Pointer Dereference	13-Aug-20	4.3	A null pointer dereference vulnerability in clj_media_size() in devices/gdevclj.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16295**	N/A	A-ART-GHOS-200820/25
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in GetNumWrongData() in contrib/lips4/gdevlips.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16296**	N/A	A-ART-GHOS-200820/26
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in FloydSteinbergDitheringC( ) in contrib/gdevbjca.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a	N/A	A-ART-GHOS-200820/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16297**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Aug-20	4.3	A buffer overflow vulnerability in mj_color_correct() in contrib/japanese/gdevmjc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16298**	N/A	A-ART-GHOS-200820/28
Divide By Zero	13-Aug-20	4.3	A Division by Zero vulnerability in bj10v_print_page() in contrib/japanese/gdev10v.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16299**	N/A	A-ART-GHOS-200820/29
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in tiff12_print_page() in devices/gdevtfnx.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16300**	N/A	A-ART-GHOS-200820/30
Buffer Copy without	13-Aug-20	4.3	A buffer overflow vulnerability in	N/A	A-ART-GHOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			okiibm_print_page1() in devices/gdevokii.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16301**		200820/31
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	13-Aug-20	6.8	A buffer overflow vulnerability in jetp3852_print_page() in devices/gdev3852.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16302**	N/A	A-ART-GHOS-200820/32
Use After Free	13-Aug-20	6.8	A use-after-free vulnerability in xps_finish_image_path() in devices/vector/gdevxps.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16303**	N/A	A-ART-GHOS-200820/33
Out-of-bounds Write	13-Aug-20	6.8	A buffer overflow vulnerability in image_render_color_thresh() in base/gxicolor.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted eps	N/A	A-ART-GHOS-200820/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file. This is fixed in v9.51. **CVE ID : CVE-2020-16304**		
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in pcx_write_rle() in contrib/japanese/gdev10v.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16305**	N/A	A-ART-GHOS-200820/35
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in p_print_image() in devices/gdevcdj.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-16308**	N/A	A-ART-GHOS-200820/36
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in lxm5700m_print_page() in devices/gdevlxm.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted eps file. This is fixed in v9.51. **CVE ID : CVE-2020-16309**	N/A	A-ART-GHOS-200820/37
Out-of-bounds Write	13-Aug-20	4.3	A buffer overflow vulnerability in GetNumSameData() in contrib/lips4/gdevlips.c of	N/A	A-ART-GHOS-200820/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51. **CVE ID : CVE-2020-17538**		
Bitdefender					
endpoint_security					
Improper Authentication	03-Aug-20	4.6	Improper Authentication vulnerability in Bitdefender Endpoint Security for Mac allows an unprivileged process to restart the main service and potentially inject third-party code into a trusted process. This issue affects: Bitdefender Endpoint Security for Mac versions prior to 4.12.80. **CVE ID : CVE-2020-8108**	N/A	A-BIT-ENDP-200820/39
calendar01_project					
calendar01					
Cross-Site Request Forgery (CSRF)	04-Aug-20	6.8	Cross-site request forgery (CSRF) vulnerability in [Calendar01] free edition ver1.0.0 and [Calendar02] free edition ver1.0.0 allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2020-5615**	N/A	A-CAL-CALE-200820/40
Improper Authentication	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01],	N/A	A-CAL-CALE-200820/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**		
calendar02_project					
calendar02					
Cross-Site Request Forgery (CSRF)	04-Aug-20	6.8	Cross-site request forgery (CSRF) vulnerability in [Calendar01] free edition ver1.0.0 and [Calendar02] free edition ver1.0.0 allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2020-5615**	N/A	A-CAL-CALE-200820/42
Improper Authenticati on	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and	N/A	A-CAL-CALE-200820/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**		
calendarform01_project					
calendarform01					
Improper Authentication	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free	N/A	A-CAL-CALE-200820/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**		
Canonical					
whoopsie					
Missing Release of Resource after Effective Lifetime	06-Aug-20	2.1	In whoopsie, parse_report() from whoopsie.c allows a local attacker to cause a denial of service via a crafted file. The DoS is caused by resource exhaustion due to a memory leak. Fixed in 0.2.52.5ubuntu0.5, 0.2.62ubuntu0.5 and 0.2.69ubuntu0.1. **CVE ID : CVE-2020-11937**	https://github.com/sungjungk/whoopsie_killer, https://launchpad.net/bugs/1881982, https://usn.ubuntu.com/4450-1	A-CAN-WHOO-200820/45
apport					
Improper Handling of Exceptional Conditions	06-Aug-20	2.1	An unhandled exception in check_ignored() in apport/report.py can be exploited by a local attacker to cause a denial of service. If the mtime attribute is a string value in apport-ignore.xml, it will trigger an unhandled exception, resulting in a crash. Fixed in 2.20.1-0ubuntu2.24, 2.20.9-0ubuntu7.16, 2.20.11-0ubuntu27.6.	https://launchpad.net/bugs/1877023, https://usn.ubuntu.com/4449-1	A-CAN-APPO-200820/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15701		
Time-of-check Time-of-use (TOCTOU) Race Condition	06-Aug-20	4.4	TOCTOU Race Condition vulnerability in apport allows a local attacker to escalate privileges and execute arbitrary code. An attacker may exit the crashed process and exploit PID recycling to spawn a root process with the same PID as the crashed process, which can then be used to escalate privileges. Fixed in 2.20.1-0ubuntu2.24, 2.20.9 versions prior to 2.20.9-0ubuntu7.16 and 2.20.11 versions prior to 2.20.11-0ubuntu27.6. Was ZDI-CAN-11234. **CVE ID : CVE-2020-15702**	https://usn.ubuntu.com/4449-1	A-CAN-APPO-200820/47
carson-saint					
saint_security_suite					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	A cross-site scripting (XSS) vulnerability in the Credential Manager component in SAINT Security Suite 8.0 through 9.8.20 could allow arbitrary script to run in the context of a logged-in user when the user clicks on a specially crafted link. **CVE ID : CVE-2020-16275**	https://download.saintcorporation.com/products/saint_advisory15.txt	A-CAR-SAIN-200820/48
Improper Neutralization of Special Elements used in an	10-Aug-20	6.5	An SQL injection vulnerability in the Assets component of SAINT Security Suite 8.0 through 9.8.20 allows a remote,	https://download.saintcorporation.com/products/saint_advisor	A-CAR-SAIN-200820/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			authenticated attacker to gain unauthorized access to the database. **CVE ID : CVE-2020-16276**	y15.txt	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Aug-20	6.5	An SQL injection vulnerability in the Analytics component of SAINT Security Suite 8.0 through 9.8.20 allows a remote, authenticated attacker to gain unauthorized access to the database. **CVE ID : CVE-2020-16277**	https://download.saintcorporation.com/products/saint_advisory15.txt	A-CAR-SAIN-200820/50
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	A cross-site scripting (XSS) vulnerability in the Permissions component in SAINT Security Suite 8.0 through 9.8.20 could allow arbitrary script to run in the context of a logged-in user when the user clicks on a specially crafted link. **CVE ID : CVE-2020-16278**	https://download.saintcorporation.com/products/saint_advisory15.txt	A-CAR-SAIN-200820/51
cayintech					
xpost					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Aug-20	10	CAYIN xPost suffers from an unauthenticated SQL Injection vulnerability. Input passed via the GET parameter 'wayfinder_seqid' in wayfinder_meeting_input.jsp is not properly sanitized before being returned to the user or used in SQL queries. This can be exploited to manipulate SQL queries by	N/A	A-CAY-XPOS-200820/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injecting arbitrary SQL code and execute SYSTEM commands. **CVE ID : CVE-2020-7356**		
chartkick_project					
chartkick					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-Aug-20	4.3	The Chartkick gem through 3.3.2 for Ruby allows Cascading Style Sheets (CSS) Injection (without attribute). **CVE ID : CVE-2020-16254**	N/A	A-CHA-CHAR-200820/53
Checkpoint					
zonealarm_anti-ransomware					
Improper Link Resolution Before File Access ('Link Following')	04-Aug-20	1.9	ZoneAlarm Anti-Ransomware before version 1.0.713 copies files for the report from a directory with low privileges. A sophisticated timed attacker can replace those files with malicious or linked content, such as exploiting CVE-2020-0896 on unpatched systems or using symbolic links. **CVE ID : CVE-2020-6012**	N/A	A-CHE-ZONE-200820/54
cohesive					
vns3					
Improper Neutralization of Special Elements used in an OS Command	04-Aug-20	9	The administrative interface of Cohesive Networks vns3:vpn appliances before version 4.11.1 is vulnerable to authenticated remote code	N/A	A-COH-VNS3-200820/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			execution leading to server compromise. **CVE ID : CVE-2020-15467**		
Combodo					
itop					
Information Exposure	10-Aug-20	5	A function in Combodo iTop contains a vulnerability of Broken Access Control, which allows unauthorized attacker to inject command and disclose system information. **CVE ID : CVE-2020-12777**	N/A	A-COM-ITOP-200820/56
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	Combodo iTop does not validate inputted parameters, attackers can inject malicious commands and launch XSS attack. **CVE ID : CVE-2020-12778**	N/A	A-COM-ITOP-200820/57
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	3.5	Combodo iTop contains a stored Cross-site Scripting vulnerability, which can be attacked by uploading file with malicious script. **CVE ID : CVE-2020-12779**	N/A	A-COM-ITOP-200820/58
Information Exposure	10-Aug-20	5	A security misconfiguration exists in Combodo iTop, which can expose sensitive information. **CVE ID : CVE-2020-12780**	N/A	A-COM-ITOP-200820/59
Cross-Site Request	10-Aug-20	6.8	Combodo iTop contains a cross-site request forgery	N/A	A-COM-ITOP-200820/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			(CSRF) vulnerability, attackers can execute specific commands via malicious site request forgery. **CVE ID : CVE-2020-12781**		
cs2-network					
p2p					
Improper Certificate Validation	10-Aug-20	6.8	CS2 Network P2P through 3.x, as used in millions of Internet of Things devices, suffers from an authentication flaw that allows remote attackers to perform a man-in-the-middle attack, as demonstrated by eavesdropping on user video/audio streams, capturing credentials, and compromising devices. **CVE ID : CVE-2020-9525**	N/A	A-CS2-P2P-200820/61
Information Exposure	10-Aug-20	4.3	CS2 Network P2P through 3.x, as used in millions of Internet of Things devices, suffers from an information exposure flaw that exposes user session data to supernodes in the network, as demonstrated by passively eavesdropping on user video/audio streams, capturing credentials, and compromising devices. **CVE ID : CVE-2020-9526**	N/A	A-CS2-P2P-200820/62
deltaww					
tpeditor					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	07-Aug-20	6.8	Delta Electronics TPEditor Versions 1.97 and prior. An out-of-bounds read may be exploited by processing specially crafted project files. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application. **CVE ID : CVE-2020-16219**	N/A	A-DEL-TPED-200820/63
Out-of-bounds Write	07-Aug-20	6.8	Delta Electronics TPEditor Versions 1.97 and prior. A stack-based buffer overflow may be exploited by processing a specially crafted project file. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application. **CVE ID : CVE-2020-16221**	N/A	A-DEL-TPED-200820/64
Out-of-bounds Write	07-Aug-20	6.8	Delta Electronics TPEditor Versions 1.97 and prior. A heap-based buffer overflow may be exploited by processing a specially crafted project file. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the	N/A	A-DEL-TPED-200820/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application. **CVE ID : CVE-2020-16223**		
Out-of-bounds Write	07-Aug-20	6.8	Delta Electronics TPEditor Versions 1.97 and prior. A write-what-where condition may be exploited by processing a specially crafted project file. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application. **CVE ID : CVE-2020-16225**	N/A	A-DEL-TPED-200820/66
Improper Input Validation	07-Aug-20	6.8	Delta Electronics TPEditor Versions 1.97 and prior. An improper input validation may be exploited by processing a specially crafted project file not validated when the data is entered by a user. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application. **CVE ID : CVE-2020-16227**	N/A	A-DEL-TPED-200820/67
cncsoft_screeneditor					
Out-of-bounds Write	04-Aug-20	6.8	Delta Industrial Automation CNCSoft ScreenEditor, Versions 1.01.23 and prior. Multiple stack-based buffer overflow vulnerabilities	N/A	A-DEL-CNCS-200820/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be exploited by processing specially crafted project files, which may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application. **CVE ID : CVE-2020-16199**		
Out-of-bounds Read	04-Aug-20	4.3	Delta Industrial Automation CNCSoft ScreenEditor, Versions 1.01.23 and prior. Multiple out-of-bounds read vulnerabilities may be exploited by processing specially crafted project files, which may allow an attacker to read information. **CVE ID : CVE-2020-16201**	N/A	A-DEL-CNCS-200820/69
Access of Uninitialized Pointer	04-Aug-20	6.8	Delta Industrial Automation CNCSoft ScreenEditor, Versions 1.01.23 and prior. An uninitialized pointer may be exploited by processing a specially crafted project file. Successful exploitation of this vulnerability may allow an attacker to read/modify information, execute arbitrary code, and/or crash the application. **CVE ID : CVE-2020-16203**	N/A	A-DEL-CNCS-200820/70
django-celery-results_project					
django-celery-results					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Storage of Sensitive Information	11-Aug-20	5	django-celery-results through 1.2.1 stores task results in the database. Among the data it stores are the variables passed into the tasks. The variables may contain sensitive cleartext information that does not belong unencrypted in the database. **CVE ID : CVE-2020-17495**	N/A	A-DJA-DJAN-200820/71
easycorp					
zentao_pro					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-20	9	The EasyCorp ZenTao Pro application suffers from an OS command injection vulnerability in its '/pro/repo-create.html' component. After authenticating to the ZenTao dashboard, attackers may construct and send arbitrary OS commands via the POST parameter 'path', and those commands will run in an elevated SYSTEM context on the underlying Windows operating system. **CVE ID : CVE-2020-7361**	N/A	A-EAS-ZENT-200820/72
etcd					
etcd					
Improper Input Validation	05-Aug-20	4	In etcd before versions 3.3.23 and 3.4.10, a large slice causes panic in decodeRecord method. The size of a record is	https://github.com/etcd-io/etcd/security/advisories/GHSA-	A-ETC-ETCD-200820/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stored in the length field of a WAL file and no additional validation is done on this data. Therefore, it is possible to forge an extremely large frame size that can unintentionally panic at the expense of any RAFT participant trying to decode the WAL. **CVE ID : CVE-2020-15106**	p4g4-wgrh-qrg2	
Improper Input Validation	05-Aug-20	4	In etcd before versions 3.3.23 and 3.4.10, it is possible to have an entry index greater then the number of entries in the ReadAll method in wal/wal.go. This could cause issues when WAL entries are being read during consensus as an arbitrary etcd consensus participant could go down from a runtime panic when reading the entry. **CVE ID : CVE-2020-15112**	https://github.com/etcd-io/etcd/security/advisories/GHSA-m332-53r6-2w93	A-ETC-ETCD-200820/74
Improper Preservation of Permissions	05-Aug-20	3.6	In etcd before versions 3.3.23 and 3.4.10, certain directory paths are created (etcd data directory and the directory path when provided to automatically generate self-signed certificates for TLS connections with clients) with restricted access permissions (700) by using the os.MkdirAll. This function does not perform	https://github.com/etcd-io/etcd/security/advisories/GHSA-chh6-ppwq-jh92	A-ETC-ETCD-200820/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			any permission checks when a given directory path exists already. A possible workaround is to ensure the directories have the desired permission (700). **CVE ID : CVE-2020-15113**		
Extremenetworks					
extreme_management_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-20	4.3	Extreme EAC Appliance 8.4.1.24 allows unauthenticated reflected XSS via a parameter in a GET request. **CVE ID : CVE-2020-13819**	https://documentation.extremenetworks.com/release_notes/netsight/XMC_8.5.0_Release_Notes.pdf	A-EXT-EXTR-200820/76
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-20	4.3	Extreme Management Center 8.4.1.24 allows unauthenticated reflected XSS via a parameter in a GET request. **CVE ID : CVE-2020-13820**	N/A	A-EXT-EXTR-200820/77
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-20	4.3	Extreme Analytics in Extreme Management Center before 8.5.0.169 allows unauthenticated reflected XSS via a parameter in a GET request, aka CFD-4887. **CVE ID : CVE-2020-16847**	N/A	A-EXT-EXTR-200820/78
f2fs-tools_project					
f2fs-tools					
Incorrect Calculation	10-Aug-20	6.8	An exploitable code execution vulnerability	N/A	A-F2F-F2FS-200820/79

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Buffer Size			exists in the file system checking functionality of fsck.f2fs 1.12.0. A specially crafted f2fs file can cause a logic flaw and out-of-bounds heap operations, resulting in code execution. An attacker can provide a malicious file to trigger this vulnerability. **CVE ID : CVE-2020-6070**		
field_test_project					
field_test					
Cross-Site Request Forgery (CSRF)	05-Aug-20	4.3	The Field Test gem 0.2.0 through 0.3.2 for Ruby allows CSRF. **CVE ID : CVE-2020-16252**	N/A	A-FIE-FIEL-200820/80
firejail_project					
firejail					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Aug-20	4.6	Firejail through 0.9.62 does not honor the -- end-of-options indicator after the --output option, which may lead to command injection. **CVE ID : CVE-2020-17367**	N/A	A-FIR-FIRE-200820/81
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Aug-20	7.5	Firejail through 0.9.62 mishandles shell metacharacters during use of the --output or --output-stderr option, which may lead to command injection. **CVE ID : CVE-2020-17368**	N/A	A-FIR-FIRE-200820/82
Flatcore					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
flatcore					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-20	3.5	flatCore before 1.5.7 allows XSS by an admin via the acp/acp.php?tn=pages&sub=edit&editpage=1 page_linkname, page_title, page_content, or page_extracontent parameter, or the acp/acp.php?tn=system&sub=sys_pref prefs_pagename, prefs_pagetitle, or prefs_pagesubtitle parameter. **CVE ID : CVE-2020-17451**	N/A	A-FLA-FLAT-200820/83
Unrestricted Upload of File with Dangerous Type	09-Aug-20	9	flatCore before 1.5.7 allows upload and execution of a .php file by an admin. **CVE ID : CVE-2020-17452**	N/A	A-FLA-FLAT-200820/84
frappe					
erpnext					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	10-Aug-20	6.5	An SQL injection vulnerability exists in the frappe.desk.reportview.get functionality of ERPNext 11.1.38. A specially crafted HTTP request can cause an SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability. **CVE ID : CVE-2020-6145**	N/A	A-FRA-ERPN-200820/85
gallery01_project					
gallery01					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**	N/A	A-GAL-GALL-200820/86
gantt-chart_project					
gantt-chart					
Missing Authorization	04-Aug-20	5.5	An issue was discovered in the Gantt-Chart module before 5.5.4 for Jira. Due to a missing privilege check, it is possible to read and write to the module configuration of other users. This can also be used to deliver an XSS payload to other users' dashboards. To exploit this vulnerability, an attacker	N/A	A-GAN-GANT-200820/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has to be authenticated. **CVE ID : CVE-2020-15943**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-20	3.5	An issue was discovered in the Gantt-Chart module before 5.5.5 for Jira. Due to missing validation of user input, it is vulnerable to a persistent XSS attack. An attacker can embed the attack vectors in the dashboard of other users. To exploit this vulnerability, an attacker has to be authenticated. **CVE ID : CVE-2020-15944**	N/A	A-GAN-GANT-200820/88
Getsymphony					
symphony_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-20	4.3	content/content.blueprintsevents.php in Symphony CMS 3.0.0 allows XSS via fields['name'] to appendSubheading. **CVE ID : CVE-2020-15071**	N/A	A-GET-SYMP-200820/89
Gitlab					
runner					
Server-Side Request Forgery (SSRF)	10-Aug-20	6.5	For GitLab Runner before 13.0.12, 13.1.6, 13.2.3, by replacing dockerd with a malicious server, the Shared Runner is susceptible to SSRF. **CVE ID : CVE-2020-13295**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13295.json	A-GIT-RUNN-200820/90
gitlab					
Improper Input	13-Aug-20	4	For GitLab before 13.0.12, 13.1.6, 13.2.3 a denial of	https://gitlab.com/gitlab	A-GIT-GITL-200820/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			service exists in the project import feature **CVE ID : CVE-2020-13281**	-org/cves/-/blob/master/2020/CVE-2020-13281.json	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Aug-20	3.5	For GitLab before 13.0.12, 13.1.6, 13.2.3 a cross-site scripting vulnerability exists in the issues list via milestone title. **CVE ID : CVE-2020-13283**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13283.json	A-GIT-GITL-200820/92
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Aug-20	3.5	For GitLab before 13.0.12, 13.1.6, 13.2.3 a cross-site scripting vulnerability exists in the issue reference number tooltip. **CVE ID : CVE-2020-13285**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13285.json	A-GIT-GITL-200820/93
Server-Side Request Forgery (SSRF)	13-Aug-20	4	For GitLab before 13.0.12, 13.1.6, 13.2.3 user controlled git configuration settings can be modified to result in Server Side Request Forgery. **CVE ID : CVE-2020-13286**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13286.json	A-GIT-GITL-200820/94
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	In GitLab before 13.0.12, 13.1.6, and 13.2.3, a stored XSS vulnerability exists in the CI/CD Jobs page **CVE ID : CVE-2020-13288**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13288.json	A-GIT-GITL-200820/95
Improper Authenticati	10-Aug-20	5.5	In GitLab before 13.0.12, 13.1.6 and 13.2.3, it is	https://gitlab.com/gitlab	A-GIT-GITL-200820/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			possible to bypass E-mail verification which is required for OAuth Flow. **CVE ID : CVE-2020-13292**	-org/cves/-/blob/master/2020/CVE-2020-13292.json	
Incorrect Type Conversion or Cast	10-Aug-20	5.5	In GitLab before 13.0.12, 13.1.6 and 13.2.3 using a branch with a hexadecimal name could override an existing hash. **CVE ID : CVE-2020-13293**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13293.json	A-GIT-GITL-200820/97
N/A	10-Aug-20	5.5	In GitLab before 13.0.12, 13.1.6 and 13.2.3, access grants were not revoked when a user revoked access to an application. **CVE ID : CVE-2020-13294**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13294.json	A-GIT-GITL-200820/98
gog					
galaxy					
Incorrect Default Permissions	06-Aug-20	7.2	The GalaxyClientService component of GOG Galaxy runs with elevated SYSTEM privileges in a Windows environment. Due to the software shipping with embedded, static RSA private key, an attacker with this key material and local user permissions can effectively send any operating system command to the service for execution in this elevated context. The service listens for such commands on a locally-bound network port, localhost:9978. A	N/A	A-GOG-GALA-200820/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Metasploit module has been published which exploits this vulnerability. This issue affects the 2.0.x branch of the software (2.0.12 and earlier) as well as the 1.2.x branch (1.2.64 and earlier). A fix was issued for the 2.0.x branch of the affected software. **CVE ID : CVE-2020-7352**		
Golang					
go					
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Aug-20	5	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary via invalid inputs. **CVE ID : CVE-2020-16845**	https://groups.google.com/forum/#!topic/golang-announce/NyPIaucMgXo	A-GOL-GO-200820/100
Google					
asylo					
Improper Restriction of Operations within the Bounds of a Memory Buffer	12-Aug-20	5.5	An arbitrary memory overwrite vulnerability in the trusted memory of Asylo exists in versions prior to 0.6.0. As the ecall_restore function fails to validate the range of the output_len pointer, an attacker can manipulate the tmp_output_len value and write to an arbitrary location in the trusted (enclave) memory. We recommend updating Asylo to version 0.6.0 or	https://github.com/google/asylo/commit/e582f36ac49ee11a21d23ad6a30c333092e0a94e	A-GOO-ASYL-200820/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			later. **CVE ID : CVE-2020-8904**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	12-Aug-20	4	A buffer length validation vulnerability in Asylo versions prior to 0.6.0 allows an attacker to read data they should not have access to. The 'enc_untrusted_recvfrom' function generates a return value which is deserialized by 'MessageReader', and copied into three different 'extents'. The length of the third 'extents' is controlled by the outside world, and not verified on copy, allowing the attacker to force Asylo to copy trusted memory data into an untrusted buffer of significantly small length.. We recommend updating Asylo to version 0.6.0 or later. **CVE ID : CVE-2020-8905**	https://github.com/google/asylo/commit/299f804acbb95a612ab7c504d25ab908aa59ae93	A-GOO-ASYL-200820/102
handysoft					
hslogin2.dll					
Improper Validation of Integrity Check Value	07-Aug-20	6.8	hslogin2.dll ActiveX Control in Groupware contains a vulnerability that could allow remote files to be downloaded and executed by setting the arguments to the activex method. This is due to a lack of integrity verification of the policy	N/A	A-HAN-HSLO-200820/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files referenced in the update process, and a remote attacker could induce a user to crafted web page, causing damage such as malicious code infection. **CVE ID : CVE-2020-7810**		
hmtalk					
daviewindy					
Out-of-bounds Write	04-Aug-20	6.8	DaviewIndy has a Heap-based overflow vulnerability, triggered when the user opens a malformed image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7822**	N/A	A-HMT-DAVI-200820/104
Improper Input Validation	04-Aug-20	6.8	DaviewIndy has a Memory corruption vulnerability, triggered when the user opens a malformed image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7823**	N/A	A-HMT-DAVI-200820/105
Huawei					
fusioncompute					
Improper Privilege Management	10-Aug-20	4.6	FusionCompute 8.0.0 have local privilege escalation vulnerability. A local, authenticated attacker could perform specific operations to exploit this vulnerability. Successful	N/A	A-HUA-FUSI-200820/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation may cause the attacker to obtain a higher privilege and compromise the service. **CVE ID : CVE-2020-9078**		
fusionsphere_openstack					
N/A	11-Aug-20	5.8	FusionSphere OpenStack 8.0.0 have a protection mechanism failure vulnerability. The product incorrectly uses a protection mechanism. An attacker has to find a way to exploit the vulnerability to conduct directed attacks against the affected product. **CVE ID : CVE-2020-9079**	N/A	A-HUA-FUSI-200820/107
IBM					
urbancode_deploy					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	05-Aug-20	6.4	IBM UrbanCode Deploy (UCD) 6.2.7.3, 6.2.7.4, 7.0.3.0, and 7.0.4.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 181848. **CVE ID : CVE-2020-4481**	https://www.ibm.com/support/pages/node/6256128	A-IBM-URBA-200820/108
i2_analysts_notebook					
Improper Restriction of	03-Aug-20	6.9	IBM i2 Analyst Notebook 9.2.1 could allow a local attacker to execute	https://www.ibm.com/support/page	A-IBM-I2_A-200820/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183317. **CVE ID : CVE-2020-4549**	s/node/6254694	
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-20	6.9	IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183318. **CVE ID : CVE-2020-4550**	https://www.ibm.com/support/pages/node/6254694	A-IBM-I2_A-200820/110
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-20	6.9	IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183319. **CVE ID : CVE-2020-4551**	https://www.ibm.com/support/pages/node/6254694	A-IBM-I2_A-200820/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-20	6.9	IBM i2 Analyst Notebook 9.2.1 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183320. **CVE ID : CVE-2020-4552**	https://www.ibm.com/support/pages/node/6254694	A-IBM-I2_A-200820/112
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-20	6.9	IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 183321. **CVE ID : CVE-2020-4553**	https://www.ibm.com/support/pages/node/6254694	A-IBM-I2_A-200820/113
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-Aug-20	6.9	IBM i2 Analyst Notebook 9.2.1 and 9.2.2 could allow a local attacker to execute arbitrary code on the system, caused by a memory corruption. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force	https://www.ibm.com/support/pages/node/6254694	A-IBM-I2_A-200820/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: 183322. **CVE ID : CVE-2020-4554**		
security_identity_governance_and_intelligence					
Session Fixation	05-Aug-20	4.3	IBM Security Identity Governance and Intelligence 5.2.6 Virtual Appliance could allow a remote attacker to obtain sensitive information using man in the middle techniques due to not properly invalidating session tokens. IBM X-Force ID: 175420. **CVE ID : CVE-2020-4243**	https://www.ibm.com/support/pages/node/6255972	A-IBM-SECU-200820/115
jazz_reporting_service					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	IBM Jazz Reporting Service 6.0.6, 6.0.6.1, and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182717. **CVE ID : CVE-2020-4533**	https://www.ibm.com/support/pages/node/6257565	A-IBM-JAZZ-200820/116
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	IBM Jazz Reporting Service 6.0.2, 6.0.6, 6.0.6.1, 7.0, and 7.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	https://www.ibm.com/support/pages/node/6257575	A-IBM-JAZZ-200820/117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially leading to credentials disclosure within a trusted session. **CVE ID : CVE-2020-4539**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	IBM Jazz Reporting Service 7.0 and 7.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 183039. **CVE ID : CVE-2020-4541**	https://www.ibm.com/support/pages/node/6257577	A-IBM-JAZZ-200820/118
rational_rhapsody_design_manager					
Information Exposure	04-Aug-20	4	IBM Jazz Foundation and IBM Engineering products could allow an authenticated user to send a specially crafted HTTP GET request to read attachments on the server that they should not have access to. IBM X-Force ID: 179539. **CVE ID : CVE-2020-4410**	https://www.ibm.com/support/pages/node/6255694	A-IBM-RATI-200820/119
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-20	3.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to	https://www.ibm.com/support/pages/node/6255694	A-IBM-RATI-200820/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials disclosure within a trusted session. IBM X-Force ID: 182435. **CVE ID : CVE-2020-4525**		
spectrum_protect_plus					
Incorrect Permission Assignment for Critical Resource	04-Aug-20	1.9	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 agent files, in non-default configurations, on Windows are assigned access to everyone with full control permissions, which could allow a local user to cause interruption of the service operations. IBM X-Force ID: 185372. **CVE ID : CVE-2020-4631**	https://www.ibm.com/support/pages/node/6255116	A-IBM-SPEC-200820/121
cognos_analytics					
Improper Restriction of Recursive Entity References in DTDs ('XML Entity Expansion')	03-Aug-20	6.4	IBM Cognos Anaytics 11.0 and 11.1 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 179156. **CVE ID : CVE-2020-4377**	https://www.ibm.com/support/pages/node/6252853	A-IBM-COGN-200820/122
security_secret_server					
Use of Hard-coded Credentials	04-Aug-20	7.5	IBM Security Verify Access 10.7 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound	https://www.ibm.com/support/pages/node/6255614	A-IBM-SECU-200820/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 181395. **CVE ID : CVE-2020-4459**		
websphere_application_server					
Improper Privilege Management	03-Aug-20	7.2	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper handling of UNC paths. By scheduling a task with a specially-crafted UNC path, an attacker could exploit this vulnerability to execute arbitrary code with higher privileges. IBM X-Force ID: 182808. **CVE ID : CVE-2020-4534**	https://www.ibm.com/support/pages/node/6255074	A-IBM-WEBS-200820/124
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	13-Aug-20	10	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. The vulnerability only occurs if an undocumented customization has been applied by an administrator. IBM X-Force ID: 184585. **CVE ID : CVE-2020-4589**	https://www.ibm.com/support/pages/node/6258333	A-IBM-WEBS-200820/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
financial_transaction_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-20	4.3	IBM Financial Transaction Manager 3.2.4 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. **CVE ID : CVE-2020-4560**	https://www.ibm.com/support/pages/node/6255190	A-IBM-FINA-200820/126
qradar_security_information_and_event_manager					
N/A	11-Aug-20	4	IBM QRadar 7.2.0 through 7.2.9 could allow an authenticated user to disable the Wincollect service which could aid an attacker in bypassing security mechanisms in future attacks. IBM X-Force ID: 181860. **CVE ID : CVE-2020-4485**	https://www.ibm.com/support/pages/node/6257885	A-IBM-QRAD-200820/127
N/A	11-Aug-20	5.5	IBM QRadar 7.2.0 thorugh 7.2.9 could allow an authenticated user to overwrite or delete arbitrary files due to a flaw after WinCollect installation. IBM X-Force ID: 181861. **CVE ID : CVE-2020-4486**	https://www.ibm.com/support/pages/node/6257885	A-IBM-QRAD-200820/128
engineering_test_management					
Improper Neutralization of Input	04-Aug-20	3.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-	https://www.ibm.com/support/page	A-IBM-ENGI-200820/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			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: 179359. **CVE ID : CVE-2020-4396**	s/node/6255694	
Information Exposure	04-Aug-20	4	IBM Jazz Foundation and IBM Engineering products could allow an authenticated user to send a specially crafted HTTP GET request to read attachments on the server that they should not have access to. IBM X-Force ID: 179539. **CVE ID : CVE-2020-4410**	https://www.ibm.com/support/pages/node/6255694	A-IBM-ENGI-200820/130
engineering_workflow_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-20	3.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 182435. **CVE ID : CVE-2020-4525**	https://www.ibm.com/support/pages/node/6255694	A-IBM-ENGI-200820/131
engineering_requirements_management_doors_next					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	04-Aug-20	3.5	IBM Jazz Foundation and IBM Engineering products are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-force ID: 183046. **CVE ID : CVE-2020-4542**	https://www.ibm.com/support/pages/node/6255694	A-IBM-ENGI-200820/132
event_streams					
Improper Authentication	14-Aug-20	6.5	IBM Event Streams 10.0.0 could allow an authenticated user to perform tasks to a schema due to improper authentication validation. IBM X-Force ID: 186233. **CVE ID : CVE-2020-4662**	https://www.ibm.com/support/pages/node/6259393	A-IBM-EVEN-200820/133
financial_transaction_manager_for_multiplatform					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	03-Aug-20	6.5	IBM Financial Transaction Manager 3.2.4 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 database. IBM X-Force ID: 177839. **CVE ID : CVE-2020-4328**	https://www.ibm.com/support/pages/node/6255154	A-IBM-FINA-200820/134
ivanti					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
desktop\&server_management					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Aug-20	10	Denial-of-Service (DoS) in Ivanti Service Manager HEAT Remote Control 7.4 due to a buffer overflow in the protocol parser of the 'HEATRemoteService' agent. The DoS can be triggered by sending a specially crafted network packet. **CVE ID : CVE-2020-12441**	N/A	A-IVA-DESK-200820/135
service_manager_heat_remote_control					
Improper Restriction of Operations within the Bounds of a Memory Buffer	06-Aug-20	10	Denial-of-Service (DoS) in Ivanti Service Manager HEAT Remote Control 7.4 due to a buffer overflow in the protocol parser of the 'HEATRemoteService' agent. The DoS can be triggered by sending a specially crafted network packet. **CVE ID : CVE-2020-12441**	N/A	A-IVA-SERV-200820/136
dsm_netinst					
Use of Hard-coded Credentials	06-Aug-20	7.5	Unsafe storage of AD credentials in Ivanti DSM netinst 5.1 due to a static, hard-coded encryption key. **CVE ID : CVE-2020-13793**	N/A	A-IVA-DSM_-200820/137
jeedom					
jeedom					
Improper Neutralization of Input During Web Page	05-Aug-20	4.3	Jeedom through 4.0.38 allows XSS. **CVE ID : CVE-2020-9036**	N/A	A-JEE-JEED-200820/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')					
Jenkins					
jenkins					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the tooltip content of help icons, resulting in a stored cross-site scripting (XSS) vulnerability. **CVE ID : CVE-2020-2229**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1955	A-JEN-JENK-200820/139
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the project naming strategy description, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Overall/Manage permission. **CVE ID : CVE-2020-2230**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1957	A-JEN-JENK-200820/140
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the remote address of the host starting a build via 'Trigger builds remotely', resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Job/Configure permission or knowledge of the Authentication Token. **CVE ID : CVE-2020-2231**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1960	A-JEN-JENK-200820/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
email_extension					
Cleartext Transmission of Sensitive Information	12-Aug-20	5	Jenkins Email Extension Plugin 2.72 and 2.73 transmits and displays the SMTP password in plain text as part of the global Jenkins configuration form, potentially resulting in its exposure. **CVE ID : CVE-2020-2232**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1975	A-JEN-EMAI-200820/142
pipeline_maven_integration					
Incorrect Authorization	12-Aug-20	4	A missing permission check in Jenkins Pipeline Maven Integration Plugin 3.8.2 and earlier allows users with Overall/Read access to enumerate credentials ID of credentials stored in Jenkins. **CVE ID : CVE-2020-2233**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1794%20(1)	A-JEN-PIPE-200820/143
Missing Authorization	12-Aug-20	4	A missing permission check in Jenkins Pipeline Maven Integration Plugin 3.8.2 and earlier allows users with Overall/Read access to connect to an attacker-specified JDBC URL using attacker-specified credentials IDs obtained through another method, potentially capturing credentials stored in Jenkins. **CVE ID : CVE-2020-2234**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1794%20(2)	A-JEN-PIPE-200820/144
Cross-Site Request Forgery	12-Aug-20	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins Pipeline Maven Integration	https://jenkins.io/security/advisory/2020-08-	A-JEN-PIPE-200820/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(CSRF)			Plugin 3.8.2 and earlier allows attackers to connect to an attacker-specified JDBC URL using attacker-specified credentials IDs obtained through another method, potentially capturing credentials stored in Jenkins. **CVE ID : CVE-2020-2235**	12/#SECURITY-1794%20(2)	
yet_another_build_visualizer					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	Jenkins Yet Another Build Visualizer Plugin 1.11 and earlier does not escape tooltip content, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Run/Update permission. **CVE ID : CVE-2020-2236**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1940	A-JEN-YET_-200820/146
flaky_test_handler					
Cross-Site Request Forgery (CSRF)	12-Aug-20	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins Flaky Test Handler Plugin 1.0.4 and earlier allows attackers to rebuild a project at a previous git revision. **CVE ID : CVE-2020-2237**	https://jenkins.io/security/advisory/2020-08-12/#SECURITY-1763	A-JEN-FLAK-200820/147
Jerryscript					
jerryscript					
Out-of-bounds Write	13-Aug-20	6.8	** DISPUTED ** JerryScript through 2.3.0 allows stack consumption via function a(){new new	N/A	A-JER-JERR-200820/148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Proxy(a,{})}JSON.parse("[]",a). NOTE: the vendor states that the problem is the lack of the --stack-limit option. **CVE ID : CVE-2020-24345**		
Jetbrains					
youtrack					
Improper Control of Generation of Code ('Code Injection')	08-Aug-20	6.5	In JetBrains YouTrack before 2020.1.1331, an external user could execute commands against arbitrary issues. **CVE ID : CVE-2020-15817**	N/A	A-JET-YOUT-200820/149
Information Exposure	08-Aug-20	5	In JetBrains YouTrack before 2020.2.8527, the subtasks workflow could disclose issue existence. **CVE ID : CVE-2020-15818**	N/A	A-JET-YOUT-200820/150
Server-Side Request Forgery (SSRF)	08-Aug-20	5	JetBrains YouTrack before 2020.2.10643 was vulnerable to SSRF that allowed scanning internal ports. **CVE ID : CVE-2020-15819**	N/A	A-JET-YOUT-200820/151
Information Exposure	08-Aug-20	5	In JetBrains YouTrack before 2020.2.6881, the markdown parser could disclose hidden file existence. **CVE ID : CVE-2020-15820**	N/A	A-JET-YOUT-200820/152
Incorrect Default Permissions	08-Aug-20	4	In JetBrains YouTrack before 2020.2.6881, a user without permission is able to create an article draft. **CVE ID : CVE-2020-15821**	N/A	A-JET-YOUT-200820/153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	08-Aug-20	5	JetBrains YouTrack before 2020.2.8873 is vulnerable to SSRF in the Workflow component. **CVE ID : CVE-2020-15823**	N/A	A-JET-YOUT-200820/154
toolbox					
Improper Verification of Cryptographic Signature	08-Aug-20	5	In JetBrains ToolBox version 1.17 before 1.17.6856, the set of signature verifications omitted the jetbrains-toolbox.exe file. **CVE ID : CVE-2020-15827**	N/A	A-JET-TOOL-200820/155
kotlin					
Improper Privilege Management	08-Aug-20	6.5	In JetBrains Kotlin from 1.4-M1 to 1.4-RC (as Kotlin 1.3.70 is not affected by the issue. Fixed version is 1.4.0) there is a script-cache privilege escalation vulnerability due to kotlin-main-kts cached scripts in the system temp directory, which is shared by all users by default. **CVE ID : CVE-2020-15824**	N/A	A-JET-KOTL-200820/156
teamcity					
Improper Privilege Management	08-Aug-20	6.5	In JetBrains TeamCity before 2020.1, users with the Modify Group permission can elevate other users' privileges. **CVE ID : CVE-2020-15825**	N/A	A-JET-TEAM-200820/157
Incorrect Authorization	08-Aug-20	4	In JetBrains TeamCity before 2020.1, users are able to assign more permissions than they	N/A	A-JET-TEAM-200820/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have. **CVE ID : CVE-2020-15826**		
Information Exposure	08-Aug-20	4	In JetBrains TeamCity before 2020.1.1, project parameter values can be retrieved by a user without appropriate permissions. **CVE ID : CVE-2020-15828**	N/A	A-JET-TEAM-200820/159
Information Exposure	08-Aug-20	5	In JetBrains TeamCity before 2019.2.3, password parameters could be disclosed via build logs. **CVE ID : CVE-2020-15829**	N/A	A-JET-TEAM-200820/160
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-20	4.3	JetBrains TeamCity before 2019.2.3 is vulnerable to stored XSS in the administration UI. **CVE ID : CVE-2020-15830**	N/A	A-JET-TEAM-200820/161
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Aug-20	4.3	JetBrains TeamCity before 2019.2.3 is vulnerable to reflected XSS in the administration UI. **CVE ID : CVE-2020-15831**	N/A	A-JET-TEAM-200820/162
json_pattern_validator_project					
json_pattern_validator					
Improper Input Validation	10-Aug-20	7.5	jpv (aka Json Pattern Validator) before 2.2.2 does not properly validate input, as demonstrated by a corrupted array.	N/A	A-JSO-JSON-200820/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-17479		
KDE					
ark					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-Aug-20	6.8	In kerfuffle/jobs.cpp in KDE Ark before 20.08.0, a crafted archive can install files outside the extraction directory via ../ directory traversal. **CVE ID : CVE-2020-16116**	https://invent.kde.org/utilities/ark/-/commit/0df592524fed305d6fbe74ddf8a196bc9ffdb92f, https://kde.org/info/security/advisory-20200730-1.txt, https://www.debian.org/security/2020/dsa-4738	A-KDE-ARK-200820/164
kee					
keepassrpc					
Use of Insufficiently Random Values	03-Aug-20	6.4	The SRP-6a implementation in Kee Vault KeePassRPC before 1.12.0 generates insufficiently random numbers, which allows remote attackers to read and modify data in the KeePass database via a WebSocket connection. **CVE ID : CVE-2020-16271**	N/A	A-KEE-KEEP-200820/165
Improper Input Validation	03-Aug-20	6.4	The SRP-6a implementation in Kee Vault KeePassRPC before 1.12.0 is missing validation for a client-provided parameter, which allows	N/A	A-KEE-KEEP-200820/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to read and modify data in the KeePass database via an A=0 WebSocket connection. **CVE ID : CVE-2020-16272**		
lilypond					
lilypond					
N/A	05-Aug-20	7.5	scm/define-stencil-commands.scm in LilyPond through 2.20.0, and 2.21.x through 2.21.4, when -dsafe is used, lacks restrictions on embedded-ps and embedded-svg, as demonstrated by including dangerous PostScript code. **CVE ID : CVE-2020-17353**	N/A	A-LIL-LILY-200820/167
Limesurvey					
limesurvey					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-20	4.3	LimeSurvey 4.3.2 allows reflected XSS because application/controllers/LSBaseController.php lacks code to validate parameters. **CVE ID : CVE-2020-16192**	N/A	A-LIM-LIME-200820/168
link01_project					
link01					
Improper Authentication	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition	N/A	A-LIN-LINK-200820/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**		
Mahara					
mahara					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-20	4.3	In Mahara 19.04 before 19.04.6, 19.10 before 19.10.4, and 20.04 before 20.04.1, certain places could execute file or folder names containing JavaScript. **CVE ID : CVE-2020-15907**	N/A	A-MAH-MAHA-200820/170
Mcafee					
total_protection					
Improper Input Validation	05-Aug-20	3.6	Unexpected behavior violation in McAfee Total Protection (MTP) prior to 16.0.R26 allows local users to turn off real time scanning via a specially crafted object making a specific function call.	N/A	A-MCA-TOTA-200820/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7298		
data_loss_prevention					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	13-Aug-20	2.3	Cross Site scripting vulnerability in McAfee Data Loss Prevention (DLP) ePO extension prior to 11.5.3 allows authenticated remote user to trigger scripts to run in a user's browser via adding a new label. **CVE ID : CVE-2020-7303**	N/A	A-MCA-DATA-200820/172
Insufficiently Protected Credentials	13-Aug-20	2.1	Unprotected Storage of Credentials vulnerability in McAfee Data Loss Prevention (DLP) for Mac prior to 11.5.2 allows local users to gain access to the RiskDB username and password via unprotected log files containing plain text credentials. **CVE ID : CVE-2020-7307**	N/A	A-MCA-DATA-200820/173
Mibew					
messenger					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	Mibew Messenger before 3.2.7 allows XSS via a crafted user name. **CVE ID : CVE-2020-17476**	N/A	A-MIB-MESS-200820/174
Microfocus					
secure_messaging_gateway					
Improper Neutralization of Special	07-Aug-20	9	DKIM key management page vulnerability on Micro Focus Secure	N/A	A-MIC-SECU-200820/175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			Messaging Gateway (SMG). Affecting all SMG Appliance running releases prior to July 2020. The vulnerability could allow a logged in user with rights to generate DKIM key information to inject system commands into the call to the DKIM system command. **CVE ID : CVE-2020-11852**		
Mozilla					
firefox					
Information Exposure	10-Aug-20	5	A Content Provider in Firefox for Android allowed local files accessible by the browser to be read by a remote webpage, leading to sensitive data disclosure, including cookies for other origins. This vulnerability affects Firefox for < Android. **CVE ID : CVE-2020-15647**	N/A	A-MOZ-FIRE-200820/176
Improper Restriction of Rendered UI Layers or Frames	10-Aug-20	4.3	Using object or embed tags, it was possible to frame other websites, even if they disallowed framing using the X-Frame-Options header. This vulnerability affects Thunderbird < 78 and Firefox < 78.0.2. **CVE ID : CVE-2020-15648**	N/A	A-MOZ-FIRE-200820/177
Improper Input Validation	10-Aug-20	4.3	A unicode RTL order character in the downloaded file name can be used to change the file's	N/A	A-MOZ-FIRE-200820/178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			name during the download UI flow to change the file extension. This vulnerability affects Firefox for iOS < 28. **CVE ID : CVE-2020-15651**		
Origin Validation Error	10-Aug-20	4.3	By observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect. This applied only to content that can be parsed as script. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1. **CVE ID : CVE-2020-15652**	N/A	A-MOZ-FIRE-200820/179
N/A	10-Aug-20	4.3	An iframe sandbox element with the allow-popups flag could be bypassed when using noopener links. This could have led to security issues for websites relying on sandbox configurations that allowed popups and hosted arbitrary content. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15653**	N/A	A-MOZ-FIRE-200820/180
Loop with Unreachable Exit Condition	10-Aug-20	4.3	When in an endless loop, a website specifying a custom cursor using CSS could make it look like the	N/A	A-MOZ-FIRE-200820/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			user is interacting with the user interface, when they are not. This could lead to a perceived broken state, especially when interactions with existing browser dialogs and warnings do not work. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15654**		
Information Exposure	10-Aug-20	4.3	A redirected HTTP request which is observed or modified through a web extension could bypass existing CORS checks, leading to potential disclosure of cross-origin information. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15655**	N/A	A-MOZ-FIRE-200820/182
Access of Resource Using Incompatible Type ('Type Confusion')	10-Aug-20	9.3	JIT optimizations involving the Javascript arguments object could confuse later optimizations. This risk was already mitigated by various precautions in the code, resulting in this bug rated at only moderate severity. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15656**	N/A	A-MOZ-FIRE-200820/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Search Path Element	10-Aug-20	6.9	Firefox could be made to load attacker-supplied DLL files from the installation directory. This required an attacker that is already capable of placing files in the installation directory. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15657**	N/A	A-MOZ-FIRE-200820/184
Improper Check for Unusual or Exceptional Conditions	10-Aug-20	4.3	The code for downloading files did not properly take care of special characters, which led to an attacker being able to cut off the file ending at an earlier position, leading to a different file type being downloaded than shown in the dialog. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15658**	N/A	A-MOZ-FIRE-200820/185
Insufficiently Protected Credentials	10-Aug-20	4.3	A rogue webpage could override the injected WKUserScript used by the logins autofill, this exploit could result in leaking a password for the current domain. This vulnerability affects Firefox for iOS < 28.	N/A	A-MOZ-FIRE-200820/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15661		
N/A	10-Aug-20	4.3	A rogue webpage could override the injected WKUserScript used by the download feature, this exploit could result in the user downloading an unintended file. This vulnerability affects Firefox for iOS < 28. **CVE ID : CVE-2020-15662**	N/A	A-MOZ-FIRE-200820/187
firefox_esr					
Unrestricted Upload of File with Dangerous Type	10-Aug-20	4.3	Given an installed malicious file picker application, an attacker was able to steal and upload local files of their choosing, regardless of the actually files picked. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.11. **CVE ID : CVE-2020-15649**	N/A	A-MOZ-FIRE-200820/188
N/A	10-Aug-20	4.3	Given an installed malicious file picker application, an attacker was able to overwrite local files and thus overwrite Firefox settings (but not access the previous profile). *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.11.	N/A	A-MOZ-FIRE-200820/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15650		
Origin Validation Error	10-Aug-20	4.3	By observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect. This applied only to content that can be parsed as script. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1. **CVE ID : CVE-2020-15652**	N/A	A-MOZ-FIRE-200820/190
N/A	10-Aug-20	4.3	An iframe sandbox element with the allow-popups flag could be bypassed when using noopener links. This could have led to security issues for websites relying on sandbox configurations that allowed popups and hosted arbitrary content. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15653**	N/A	A-MOZ-FIRE-200820/191
Loop with Unreachable Exit Condition ('Infinite Loop')	10-Aug-20	4.3	When in an endless loop, a website specifying a custom cursor using CSS could make it look like the user is interacting with the user interface, when they are not. This could lead to a perceived broken state, especially when interactions with existing	N/A	A-MOZ-FIRE-200820/192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			browser dialogs and warnings do not work. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15654**		
Information Exposure	10-Aug-20	4.3	A redirected HTTP request which is observed or modified through a web extension could bypass existing CORS checks, leading to potential disclosure of cross-origin information. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15655**	N/A	A-MOZ-FIRE-200820/193
Access of Resource Using Incompatible Type ('Type Confusion')	10-Aug-20	9.3	JIT optimizations involving the Javascript arguments object could confuse later optimizations. This risk was already mitigated by various precautions in the code, resulting in this bug rated at only moderate severity. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15656**	N/A	A-MOZ-FIRE-200820/194
Uncontrolled Search Path Element	10-Aug-20	6.9	Firefox could be made to load attacker-supplied DLL files from the installation directory. This required an attacker that is already capable of placing files in	N/A	A-MOZ-FIRE-200820/195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the installation directory. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15657**		
Improper Check for Unusual or Exceptional Conditions	10-Aug-20	4.3	The code for downloading files did not properly take care of special characters, which led to an attacker being able to cut off the file ending at an earlier position, leading to a different file type being downloaded than shown in the dialog. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15658**	N/A	A-MOZ-FIRE-200820/196
thunderbird					
Improper Restriction of Rendered UI Layers or Frames	10-Aug-20	4.3	Using object or embed tags, it was possible to frame other websites, even if they disallowed framing using the X-Frame-Options header. This vulnerability affects Thunderbird < 78 and Firefox < 78.0.2. **CVE ID : CVE-2020-15648**	N/A	A-MOZ-THUN-200820/197
Origin Validation Error	10-Aug-20	4.3	By observing the stack trace for JavaScript errors in web workers, it was	N/A	A-MOZ-THUN-200820/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possible to leak the result of a cross-origin redirect. This applied only to content that can be parsed as script. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1. **CVE ID : CVE-2020-15652**		
N/A	10-Aug-20	4.3	An iframe sandbox element with the allow-popups flag could be bypassed when using noopener links. This could have led to security issues for websites relying on sandbox configurations that allowed popups and hosted arbitrary content. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15653**	N/A	A-MOZ-THUN-200820/199
Loop with Unreachable Exit Condition ('Infinite Loop')	10-Aug-20	4.3	When in an endless loop, a website specifying a custom cursor using CSS could make it look like the user is interacting with the user interface, when they are not. This could lead to a perceived broken state, especially when interactions with existing browser dialogs and warnings do not work. This vulnerability affects Firefox ESR < 78.1, Firefox	N/A	A-MOZ-THUN-200820/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			< 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15654**		
Information Exposure	10-Aug-20	4.3	A redirected HTTP request which is observed or modified through a web extension could bypass existing CORS checks, leading to potential disclosure of cross-origin information. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15655**	N/A	A-MOZ-THUN-200820/201
Access of Resource Using Incompatible Type ('Type Confusion')	10-Aug-20	9.3	JIT optimizations involving the Javascript arguments object could confuse later optimizations. This risk was already mitigated by various precautions in the code, resulting in this bug rated at only moderate severity. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15656**	N/A	A-MOZ-THUN-200820/202
Uncontrolled Search Path Element	10-Aug-20	6.9	Firefox could be made to load attacker-supplied DLL files from the installation directory. This required an attacker that is already capable of placing files in the installation directory. *Note: This issue only affected Windows operating systems. Other	N/A	A-MOZ-THUN-200820/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating systems are unaffected.*. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15657**		
Improper Check for Unusual or Exceptional Conditions	10-Aug-20	4.3	The code for downloading files did not properly take care of special characters, which led to an attacker being able to cut off the file ending at an earlier position, leading to a different file type being downloaded than shown in the dialog. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15658**	N/A	A-MOZ-THUN-200820/204
Mybb					
mybb					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	In MyBB before version 1.8.24, the custom MyCode (BBCode) for the visual editor doesn't escape input properly when rendering HTML, resulting in a DOM-based XSS vulnerability. The weakness can be exploited by pointing a victim to a page where the visual editor is active (e.g. as a post or Private Message) and operates on a maliciously crafted MyCode message. This	https://github.com/mybb/mybb/security/advisories/GHSA-37h7-vfv6-f8rj	A-MYB-MYBB-200820/205

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may occur on pages where message content is pre-filled using a GET/POST parameter, or on reply pages where a previously saved malicious message is quoted. After upgrading MyBB to 1.8.24, make sure to update the version attribute in the `codebuttons` template for non-default themes to serve the latest version of the patched `jscripts/bbcodes_sceditor.js` file. **CVE ID : CVE-2020-15139**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-Aug-20	4.3	MyBB before 1.8.24 allows XSS because the visual editor mishandles [align], [size], [quote], and [font] in MyCode. **CVE ID : CVE-2020-17447**	N/A	A-MYB-MYBB-200820/206
nebulab					
solidus					
Improper Input Validation	04-Aug-20	5	In solidus before versions 2.8.6, 2.9.6, and 2.10.2, there is an bility to change order address without triggering address validations. This vulnerability allows a malicious customer to craft request data with parameters that allow changing the address of the current order without changing the shipment	https://github.com/solidusio/solidus/security/advisories/GHSA-3mvg-rrrw-m7ph	A-NEB-SOLI-200820/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			costs associated with the new shipment. All stores with at least two shipping zones and different costs of shipment per zone are impacted. This problem comes from how checkout permitted attributes are structured. We have a single list of attributes that are permitted across the whole checkout, no matter the step that is being submitted. See the linked reference for more information. As a workaround, if it is not possible to upgrade to a supported patched version, please use this gist in the references section. **CVE ID : CVE-2020-15109**		
Netapp					
active_iq_unified_manager					
N/A	03-Aug-20	4.6	Active IQ Unified Manager for Linux versions prior to 9.6 ship with the Java Management Extension Remote Method Invocation (JMX RMI) service enabled allowing unauthorized code execution to local users. **CVE ID : CVE-2020-8574**	N/A	A-NET-ACTI-200820/208
N/A	03-Aug-20	2.1	Active IQ Unified Manager for VMware vSphere and Windows versions prior to 9.5 are susceptible to a	N/A	A-NET-ACTI-200820/209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability which allows administrative users to cause Denial of Service (DoS). **CVE ID : CVE-2020-8575**		
Nextcloud					
nextcloud					
Improper Control of Generation of Code ('Code Injection')	10-Aug-20	4.6	A code injection in Nextcloud Desktop Client 2.6.4 allowed to load arbitrary code when placing a malicious OpenSSL config into a fixed directory. **CVE ID : CVE-2020-8224**	N/A	A-NEX-NEXT-200820/210
Uncontrolled Resource Consumption	10-Aug-20	4.9	A memory leak in the OCUtil.dll library used by Nextcloud Desktop Client 2.6.4 can lead to a DoS against the host system. **CVE ID : CVE-2020-8229**	N/A	A-NEX-NEXT-200820/211
Nginx					
njs					
Use After Free	13-Aug-20	6.8	njs through 0.4.3, used in NGINX, has a use-after-free in njs_json_parse_iterator_call in njs_json.c. **CVE ID : CVE-2020-24346**	N/A	A-NGI-NJS-200820/212
Nlnetlabs					
routinator					
Improper Certificate Validation	05-Aug-20	5.8	An issue was discovered in NLnet Labs Routinator 0.1.0 through 0.7.1. It allows remote attackers to bypass intended access restrictions or to cause a	N/A	A-NLN-ROUT-200820/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service on dependent routing systems by strategically withholding RPKI Route Origin Authorisation ".roa" files or X509 Certificate Revocation List files from the RPKI relying party's view. **CVE ID : CVE-2020-17366**		
Opensuse					
tumbleweed					
Incorrect Default Permissions	07-Aug-20	7.2	A Incorrect Default Permissions vulnerability in the packaging of inn in openSUSE Leap 15.2, openSUSE Tumbleweed, openSUSE Leap 15.1 allows local attackers with control of the new user to escalate their privileges to root. This issue affects: openSUSE Leap 15.2 inn version 2.6.2-lp152.1.26 and prior versions. openSUSE Tumbleweed inn version 2.6.2-4.2 and prior versions. openSUSE Leap 15.1 inn version 2.5.4-lp151.3.3.1 and prior versions. **CVE ID : CVE-2020-8026**	https://bugzilla.suse.com/show_bug.cgi?id=1172573	A-OPE-TUMB-200820/214
p5-crypt-perl_project					
p5-crypt-perl					
Information Exposure Through Discrepancy	10-Aug-20	5	ECDSA/EC/Point.pm in Crypt::Perl before 0.33 does not properly consider timing attacks against the EC point multiplication	N/A	A-P5--P5-C-200820/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			algorithm. **CVE ID : CVE-2020-17478**		
pactware					
pactware					
Insufficiently Protected Credentials	11-Aug-20	2.1	In PACTware before 4.1 SP6 and 5.x before 5.0.5.31, passwords are stored in a recoverable format, and may be retrieved by any user with access to the PACTware workstation. **CVE ID : CVE-2020-9403**	https://pactware.com/fileadmin/user_upload/Cyber-Security-Documents/2020-05-29_published_PWC_CyberSecurityNotifications-CVE-2020-9403-9404__002_.pdf	A-PAC-PACT-200820/216
passmark					
burnintest					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-20	7.2	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The driver's IOCTL request handler attempts to copy the input buffer onto the stack without checking its size and can cause a buffer overflow. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys. **CVE ID : CVE-2020-15479**	N/A	A-PAS-BURN-200820/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	07-Aug-20	7.2	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The kernel driver exposes IOCTL functionality that allows low-privilege users to map arbitrary physical memory into the address space of the calling process. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys. **CVE ID : CVE-2020-15480**	N/A	A-PAS-BURN-200820/218
osforensics					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-20	7.2	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The driver's IOCTL request handler attempts to copy the input buffer onto the stack without checking its size and can cause a buffer overflow. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys. **CVE ID : CVE-2020-15479**	N/A	A-PAS-OSFO-200820/219
Improper Restriction of	07-Aug-20	7.2	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics	N/A	A-PAS-OSFO-200820/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			through 7.1, and PerformanceTest through 10. The kernel driver exposes IOCTL functionality that allows low-privilege users to map arbitrary physical memory into the address space of the calling process. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys. **CVE ID : CVE-2020-15480**		
performancetest					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Aug-20	7.2	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The driver's IOCTL request handler attempts to copy the input buffer onto the stack without checking its size and can cause a buffer overflow. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys. **CVE ID : CVE-2020-15479**	N/A	A-PAS-PERF-200820/221
Improper Restriction of Operations within the Bounds of a	07-Aug-20	7.2	An issue was discovered in PassMark BurnInTest through 9.1, OSForensics through 7.1, and PerformanceTest through 10. The kernel driver	N/A	A-PAS-PERF-200820/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			exposes IOCTL functionality that allows low-privilege users to map arbitrary physical memory into the address space of the calling process. This could lead to arbitrary Ring-0 code execution and escalation of privileges. This affects DirectIo32.sys and DirectIo64.sys. **CVE ID : CVE-2020-15480**		
pghero_project					
pghero					
Cross-Site Request Forgery (CSRF)	05-Aug-20	5.8	The PgHero gem through 2.6.0 for Ruby allows CSRF. **CVE ID : CVE-2020-16253**	N/A	A-PGH-PGHE-200820/223
Php-fusion					
php-fusion					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	PHP-Fusion 9.03 allows XSS via the error_log file. **CVE ID : CVE-2020-17449**	N/A	A-PHP-PHP--200820/224
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	4.3	PHP-Fusion 9.03 allows XSS on the preview page. **CVE ID : CVE-2020-17450**	N/A	A-PHP-PHP--200820/225
pkobo-news01_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pkobo-news01					
Improper Authentication	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**	N/A	A-PKO-PKOB-200820/226
pkobo-vote01_project					
pkobo-vote01					
Improper Authentication	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01]	N/A	A-PKO-PKOB-200820/227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0, [Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**		
Plesk					
obsidian					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-20	4.3	A GET-based XSS reflected vulnerability in Plesk Obsidian 18.0.17 allows remote unauthenticated users to inject arbitrary JavaScript, HTML, or CSS via a GET parameter. **CVE ID : CVE-2020-11583**	N/A	A-PLE-OBSI-200820/228
onyx					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-20	4.3	A GET-based XSS reflected vulnerability in Plesk Onyx 17.8.11 allows remote unauthenticated users to inject arbitrary JavaScript, HTML, or CSS via a GET parameter. **CVE ID : CVE-2020-11584**	N/A	A-PLE-ONYX-200820/229
projectcontour					
contour					
Missing Authenticati	05-Aug-20	5	In Contour (Ingress controller for Kubernetes)	https://github.com/projec	A-PRO-CONT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on for Critical Function			before version 1.7.0, a bad actor can shut down all instances of Envoy, essentially killing the entire ingress data plane. GET requests to /shutdown on port 8090 of the Envoy pod initiate Envoy's shutdown procedure. The shutdown procedure includes flipping the readiness endpoint to false, which removes Envoy from the routing pool. When running Envoy (For example on the host network, pod spec hostNetwork=true), the shutdown manager's endpoint is accessible to anyone on the network that can reach the Kubernetes node that's running Envoy. There is no authentication in place that prevents a rogue actor on the network from shutting down Envoy via the shutdown manager endpoint. Successful exploitation of this issue will lead to bad actors shutting down all instances of Envoy, essentially killing the entire ingress data plane. This is fixed in version 1.7.0. **CVE ID : CVE-2020-15127**	tcontour/contour/security/advisories/GHSA-mjp8-x484-pm3r	200820/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
prometheus					
blackbox_exporter					
Server-Side Request Forgery (SSRF)	09-Aug-20	5	** DISPUTED ** Prometheus Blackbox Exporter through 0.17.0 allows /probe?target= SSRF. NOTE: follow-on discussion suggests that this might plausibly be interpreted as both intended functionality and also a vulnerability. **CVE ID : CVE-2020-16248**	N/A	A-PRO-BLAC-200820/231
Qemu					
qemu					
Improper Input Validation	11-Aug-20	5	In QEMU through 5.0.0, an assertion failure can occur in the network packet processing. This issue affects the e1000e and vmxnet3 network devices. A malicious guest user/process could use this flaw to abort the QEMU process on the host, resulting in a denial of service condition in net_tx_pkt_add_raw_fragment in hw/net/net_tx_pkt.c. **CVE ID : CVE-2020-16092**	N/A	A-QEM-QEMU-200820/232
quadra-informatique					
atos\/sips					
Improper Neutralization of Special Elements used in an OS Command	05-Aug-20	9	The ATOS/Sips (aka Atos-Magento) community module 3.0.0 to 3.0.5 for Magento allows command injection.	N/A	A-QUA-ATOS-200820/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			**CVE ID : CVE-2020-13404**		
Radare					
radare2					
Improper Input Validation	03-Aug-20	4.3	radare2 4.5.0 misparses DWARF information in executable files, causing a segmentation fault in parse_typedef in type_dwarf.c via a malformed DW_AT_name in the .debug_info section. **CVE ID : CVE-2020-16269**	N/A	A-RAD-RADA-200820/234
raonwiz					
k_upload					
Download of Code Without Integrity Check	06-Aug-20	4.6	MyBrowserPlus downloads the files needed to run the program through the setup file (Setup.inf). At this time, there is a vulnerability in downloading arbitrary files due to insufficient integrity verification of the files. **CVE ID : CVE-2020-7817**	N/A	A-RAO-K_UP-200820/235
Redhat					
cloudforms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-20	3.5	A cross-site scripting flaw was found in Report Menu feature of Red Hat CloudForms 4.7 and 5. An attacker could use this flaw to execute a stored XSS attack on an application administrator	N/A	A-RED-CLOU-200820/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using CloudForms. **CVE ID : CVE-2020-10777**		
Incorrect Authorization	11-Aug-20	6.5	In Red Hat CloudForms 4.7 and 5, the read only widgets can be edited by inspecting the forms and dropping the disabled attribute from the fields since there is no server-side validation. This business logic flaw violate the expected behavior. **CVE ID : CVE-2020-10778**	N/A	A-RED-CLOU-200820/237
Missing Authorization	11-Aug-20	4	Red Hat CloudForms 4.7 and 5 leads to insecure direct object references (IDOR) and functional level access control bypass due to missing privilege check. Therefore, if an attacker knows the right criteria, it is possible to access some sensitive data within the CloudForms. **CVE ID : CVE-2020-10779**	N/A	A-RED-CLOU-200820/238
Incorrect Authorization	11-Aug-20	6.5	Red Hat CloudForms 4.7 and 5 is affected by a role-based privilege escalation flaw. An attacker with EVM-Operator group can perform actions restricted only to EVM-Super-administrator group, leads to, exporting or importing administrator files. **CVE ID : CVE-2020-10783**	N/A	A-RED-CLOU-200820/239
Incorrect Authorizatio	11-Aug-20	6.4	Red Hat CloudForms before 5.11.7.0 was vulnerable to the User	N/A	A-RED-CLOU-200820/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			Impersonation authorization flaw which allows malicious attacker to create existent and non-existent role-based access control user, with groups and roles. With a selected group of EvmGroup-super_administrator, an attacker can perform any API request as a super administrator. **CVE ID : CVE-2020-14325**		
quay					
Information Exposure	11-Aug-20	5	An information disclosure vulnerability was found in Red Hat Quay in versions before 3.3.1. This flaw allows an attacker who can create a build trigger in a repository, to disclose the names of robot accounts and the existence of private repositories within any namespace. **CVE ID : CVE-2020-14313**	N/A	A-RED-QUAY-200820/241
amq_online					
Cross-Site Request Forgery (CSRF)	03-Aug-20	4	It was found that the AMQ Online console is vulnerable to a Cross-Site Request Forgery (CSRF) which is exploitable in cases where preflight checks are not instigated or bypassed. For example authorised users using an older browser with Adobe Flash are vulnerable when targeted by an attacker.	N/A	A-RED-AMQ_-200820/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This flaw affects all versions of AMQ-Online prior to 1.5.2 and Enmasse versions 0.31.0-rc1 up until but not including 0.32.2. **CVE ID : CVE-2020-14319**		
enmasse					
Cross-Site Request Forgery (CSRF)	03-Aug-20	4	It was found that the AMQ Online console is vulnerable to a Cross-Site Request Forgery (CSRF) which is exploitable in cases where preflight checks are not instigated or bypassed. For example authorised users using an older browser with Adobe Flash are vulnerable when targeted by an attacker. This flaw affects all versions of AMQ-Online prior to 1.5.2 and Enmasse versions 0.31.0-rc1 up until but not including 0.32.2. **CVE ID : CVE-2020-14319**	N/A	A-RED-ENMA-200820/243
etcd					
Uncontrolled Resource Consumption	06-Aug-20	4	In etcd before versions 3.3.23 and 3.4.10, the etcd gateway is a simple TCP proxy to allow for basic service discovery and access. However, it is possible to include the gateway address as an endpoint. This results in a denial of service, since the endpoint can become	https://github.com/etcd-io/etcd/security/advisories/GHSA-2xhq-gv6c-p224	A-RED-ETCD-200820/244

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stuck in a loop of requesting itself until there are no more available file descriptors to accept connections on the gateway. **CVE ID : CVE-2020-15114**		
Weak Password Requirements	06-Aug-20	5	etcd before versions 3.3.23 and 3.4.10 does not perform any password length validation, which allows for very short passwords, such as those with a length of one. This may allow an attacker to guess or brute-force users' passwords with little computational effort. **CVE ID : CVE-2020-15115**	https://github.com/etcd-io/etcd/security/advisories/GHSA-4993-m7g5-r9hh	A-RED-ETCD-200820/245
Improper Authentication	06-Aug-20	5.8	In ectd before versions 3.4.10 and 3.3.23, gateway TLS authentication is only applied to endpoints detected in DNS SRV records. When starting a gateway, TLS authentication will only be attempted on endpoints identified in DNS SRV records for a given domain, which occurs in the discoverEndpoints function. No authentication is performed against endpoints provided in the --endpoints flag. This has been fixed in versions 3.4.10 and 3.3.23 with improved documentation	https://github.com/etcd-io/etcd/security/advisories/GHSA-wr2v-9rpq-c35q	A-RED-ETCD-200820/246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and deprecation of the functionality. **CVE ID : CVE-2020-15136**		
cloudforms_management_engine					
Improper Input Validation	11-Aug-20	6.8	Red Hat CloudForms 4.7 and 5 is affected by CSV Injection flaw, a crafted payload stays dormant till a victim export as CSV and opens the file with Excel. Once the victim opens the file, the formula executes, triggering any number of possible events. While this is strictly not an flaw that affects the application directly, attackers could use the loosely validated parameters to trigger several attack possibilities. **CVE ID : CVE-2020-10780**	N/A	A-RED-CLOU-200820/247
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Aug-20	6.5	A high severity vulnerability was found in all active versions of Red Hat CloudForms before 5.11.7.0. The out of band OS command injection vulnerability can be exploited by authenticated attacker while setuping conversion host through Infrastructure Migration Solution. This flaw allows attacker to execute arbitrary commands on CloudForms server. **CVE ID : CVE-2020-14324**	N/A	A-RED-CLOU-200820/248
Server-Side Request	11-Aug-20	5.5	Red Hat CloudForms 4.7 and 5 was vulnerable to	N/A	A-RED-CLOU-200820/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			Server-Side Request Forgery (SSRF) flaw. With the access to add Ansible Tower provider, an attacker could scan and attack systems from the internal network which are not normally accessible. **CVE ID : CVE-2020-14296**		
robotemi					
temi					
Use of Hard-coded Credentials	11-Aug-20	7.5	Use of Hard-coded Credentials in Robotemi Global Ltd Temi Firmware up to 20190419.165201, Launcher OS prior to 11969-13146, Robox OS prior to 117.21-119.24, and their Android phone app prior to 1.3.3-1.3.7931 allows remote attackers to gain raised privileges on the temi and have it automatically answer the attacker's calls, granting audio, video, and motor control. **CVE ID : CVE-2020-16170**	N/A	A-ROB-TEMI-200820/250
Roundcube					
webmail					
Improper Neutralization of Input During Web Page Generation ('Cross-site	12-Aug-20	4.3	Roundcube Webmail before 1.4.8 allows stored XSS in HTML messages during message display via a crafted SVG document. **CVE ID : CVE-2020-16145**	https://github.com/roundcube/roundcubemail/commit/a71bf2e8d4a64ff2c83fdabc1e8cb	A-ROU-WEBM-200820/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				0c045a41ef4	
sabnzbd					
sabnzbd					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Aug-20	6.5	SABnzbd 2.3.9 and 3.0.0Alpha2 has a command injection vulnerability in the web configuration interface that permits an authenticated user to execute arbitrary Python commands on the underlying operating system. **CVE ID : CVE-2020-13124**	https://github.com/sabnzbd/sabnzbd/security/advisories/GHSA-9x87-96gg-33w2	A-SAB-SABN-200820/252
SAP					
abap_platform					
Improper Control of Generation of Code ('Code Injection')	12-Aug-20	6.5	SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 753, 755, allows an attacker to inject code that can be executed by the application, leading to Code Injection. An attacker could thereby control the behavior of the application. **CVE ID : CVE-2020-6296**	N/A	A-SAP-ABAP-200820/253
Information Exposure	12-Aug-20	4	SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 740, 750, 751, 752, 753, 754, 755, allows a business user to access the list of users in the given system	N/A	A-SAP-ABAP-200820/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			using value help, leading to Information Disclosure. **CVE ID : CVE-2020-6299**		
Information Exposure	12-Aug-20	4	Improper access control in SOA Configuration Trace component in SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 702, 730, 731, 740, 750, allows any authenticated user to enumerate all SAP users, leading to Information Disclosure. **CVE ID : CVE-2020-6310**	N/A	A-SAP-ABAP-200820/255
netweaver_knowledge_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	8.5	SAP NetWeaver (Knowledge Management), versions - 7.30, 7.31, 7.40, 7.50, allows the automatic execution of script content in a stored file due to inadequate filtering with the accessing user's privileges. If the accessing user has administrative privileges, then the execution of the script content could result in complete compromise of system confidentiality, integrity and availability, leading to Stored Cross Site Scripting. **CVE ID : CVE-2020-6284**	N/A	A-SAP-NETW-200820/256
Unrestricted Upload of File with Dangerous	12-Aug-20	6.4	SAP NetWeaver (Knowledge Management), versions - 7.30, 7.31, 7.40, 7.50, allows an	N/A	A-SAP-NETW-200820/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			unauthenticated attacker to upload a malicious file and also to access, modify or make unavailable existing files but the impact is limited to the files themselves and is restricted by other policies such as access control lists and other upload file size restrictions, leading to Unrestricted File Upload. **CVE ID : CVE-2020-6293**		
adaptive_server_enterprise					
Information Exposure	12-Aug-20	4.6	Under certain conditions the SAP Adaptive Server Enterprise, version 16.0, allows an attacker to access encrypted sensitive and confidential information through publicly readable installation log files leading to a compromise of the installed Cockpit. This compromise could enable the attacker to view, modify and/or make unavailable any data associated with the Cockpit, leading to Information Disclosure. **CVE ID : CVE-2020-6295**	N/A	A-SAP-ADAP-200820/258
netweaver					
Improper Authentication	12-Aug-20	7.8	SAP NetWeaver AS JAVA, versions - (ENGINEAPI 7.10; WSRM 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50; J2EE-FRMW 7.10, 7.11),	N/A	A-SAP-NETW-200820/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not perform any authentication checks for a web service allowing the attacker to send several payloads and leading to complete denial of service. **CVE ID : CVE-2020-6309**		
netweaver_as_abap					
Improper Control of Generation of Code ('Code Injection')	12-Aug-20	6.5	SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 753, 755, allows an attacker to inject code that can be executed by the application, leading to Code Injection. An attacker could thereby control the behavior of the application. **CVE ID : CVE-2020-6296**	N/A	A-SAP-NETW-200820/260
Information Exposure	12-Aug-20	4	SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 740, 750, 751, 752, 753, 754, 755, allows a business user to access the list of users in the given system using value help, leading to Information Disclosure. **CVE ID : CVE-2020-6299**	N/A	A-SAP-NETW-200820/261
Information Exposure	12-Aug-20	4	Improper access control in SOA Configuration Trace component in SAP NetWeaver (ABAP Server) and ABAP Platform, versions - 702, 730, 731, 740, 750, allows any	N/A	A-SAP-NETW-200820/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to enumerate all SAP users, leading to Information Disclosure. **CVE ID : CVE-2020-6310**		
businessobjects_business_intelligence_platform					
Missing Authentication for Critical Function	12-Aug-20	6.4	Xvfb of SAP Business Objects Business Intelligence Platform, versions - 4.2, 4.3, platform on Unix does not perform any authentication checks for functionalities that require user identity. **CVE ID : CVE-2020-6294**	N/A	A-SAP-BUSI-200820/263
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	SAP Business Objects Business Intelligence Platform (Central Management Console), versions- 4.2, 4.3, allows an attacker with administrator rights can use the web application to send malicious code to a different end user (victim), as it does not sufficiently encode user-controlled inputs for RecycleBin, resulting in Stored Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2020-6300**	N/A	A-SAP-BUSI-200820/264
s\/4_hana_fiori_ui_for_general_ledger_accounting					
Missing Authorization	12-Aug-20	4	SAP S/4 HANA (Fiori UI for General Ledger Accounting), versions 103, 104, does not perform necessary authorization	N/A	A-SAP-S\/4-200820/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks for an authenticated user working with attachment service, allowing the attacker to delete attachments due to Missing Authorization Check. **CVE ID : CVE-2020-6273**		
data_intelligence					
Information Exposure	12-Aug-20	2.1	Under certain conditions the upgrade of SAP Data Hub 2.7 to SAP Data Intelligence, version - 3.0, allows an attacker to access confidential system configuration information, that should otherwise be restricted, leading to Information Disclosure. **CVE ID : CVE-2020-6297**	N/A	A-SAP-DATA-200820/266
generic_market_data					
Missing Authorization	12-Aug-20	5.5	SAP Banking Services (Generic Market Data), versions - 400, 450, 500, allows an unauthorized user to display protected Business Partner Generic Market Data (GMD) and change related GMD key figure values, due to Missing Authorization Check. **CVE ID : CVE-2020-6298**	N/A	A-SAP-GENE-200820/267
hcm_travel_management					
Missing Authorization	12-Aug-20	5.5	SAP ERP (HCM Travel Management), versions - 600, 602, 603, 604, 605,	N/A	A-SAP-HCM_-200820/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			606, 607, 608, allows an authenticated but unauthorized attacker to read, modify and settle trips, resulting in escalation of privileges, due to Missing Authorization Check. **CVE ID : CVE-2020-6301**		
save-server_project					
save-server					
Cross-Site Request Forgery (CSRF)	04-Aug-20	6.8	save-server (npm package) before version 1.05 is affected by a CSRF vulnerability, as there is no CSRF mitigation (Tokens etc.). The fix introduced in version version 1.05 unintentionally breaks uploading so version v1.0.7 is the fixed version. This is patched by implementing Double submit. The CSRF attack would require you to navigate to a malicious site while you have an active session with Save-Server (Session key stored in cookies). The malicious user would then be able to perform some actions, including uploading/deleting files and adding redirects. If you are logged in as root, this attack is significantly more severe. They can in addition create, delete and update users. If they	https://github.com/Neztore/save-server/security/advisories/GHSA-wwrj-35w6-77ff	A-SAV-SAVE-200820/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			updated the password of a user, that user's files would then be available. If the root password is updated, all files would be visible if they logged in with the new password. Note that due to the same origin policy malicious actors cannot view the gallery or the response of any of the methods, nor be sure they succeeded. This issue has been patched in version 1.0.7. **CVE ID : CVE-2020-15135**		
securenvoy					
securmail					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Aug-20	9.3	SecurEnvoy SecurMail 9.3.503 allows attackers to upload executable files and achieve OS command execution via a crafted SecurEnvoyReply cookie. **CVE ID : CVE-2020-13376**	N/A	A-SEC-SECU-200820/270
Skygroup					
skysea_client_view					
Improper Privilege Management	04-Aug-20	4.6	Privilege escalation vulnerability in SKYSEA Client View Ver.12.200.12n to 15.210.05f allows an attacker to obtain unauthorized privileges and modify/obtain sensitive information or perform unintended operations via unspecified	N/A	A-SKY-SKYS-200820/271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vectors. **CVE ID : CVE-2020-5617**		
softperfect					
ram_disk					
Improper Input Validation	04-Aug-20	3.6	An exploitable arbitrary file delete vulnerability exists in SoftPerfect RAM Disk 4.1 spvve.sys driver. A specially crafted I/O request packet (IRP) can allow an unprivileged user to delete any file on the filesystem. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13522**	N/A	A-SOF-RAM_-200820/272
Information Exposure	04-Aug-20	2.1	An exploitable information disclosure vulnerability exists in SoftPerfect's RAM Disk 4.1 spvve.sys driver. A specially crafted I/O request packet (IRP) can cause the disclosure of sensitive information. An attacker can send a malicious IRP to trigger this vulnerability. **CVE ID : CVE-2020-13523**	N/A	A-SOF-RAM_-200820/273
soplanning					
soplanning					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-20	3.5	SOPlanning 1.46.01 allows persistent XSS via the Project Name, Statutes Comment, Places Comment, or Resources Comment field. **CVE ID : CVE-2020-15597**	N/A	A-SOP-SOPL-200820/274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sugarcrm					
sugarcrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Aug-20	3.5	SugarCRM before 10.1.0 (Q3 2020) allows XSS. **CVE ID : CVE-2020-17372**	N/A	A-SUG-SUGA-200820/275
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	12-Aug-20	3.5	SugarCRM before 10.1.0 (Q3 2020) allows SQL Injection. **CVE ID : CVE-2020-17373**	N/A	A-SUG-SUGA-200820/276
sulu					
sulu					
Information Exposure Through an Error Message	05-Aug-20	5	In Sulu before versions 1.6.35, 2.0.10, and 2.1.1, when the "Forget password" feature on the login screen is used, Sulu asks the user for a username or email address. If the given string is not found, a response with a `400` error code is returned, along with a error message saying that this user name does not exist. This enables attackers to retrieve valid usernames. Also, the response of the "Forgot Password" request returns	https://github.com/sulu/sulu/security/advisories/GHSA-wfm4-pq59-wg6r	A-SUL-SULU-200820/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the email address to which the email was sent, if the operation was successful. This information should not be exposed, as it can be used to gather email addresses. This problem was fixed in versions 1.6.35, 2.0.10 and 2.1.1. **CVE ID : CVE-2020-15132**		
Telegram					
telegram_desktop					
Incorrect Authorization	11-Aug-20	6.8	Telegram Desktop through 2.1.13 allows a spoofed file type to bypass the Dangerous File Type Execution protection mechanism, as demonstrated by use of the chat window with a filename that lacks an extension. **CVE ID : CVE-2020-17448**	N/A	A-TEL-TELE-200820/278
telop01_project					
telop01					
Improper Authentication	04-Aug-20	7.5	[Calendar01], [Calendar02], [PKOBO-News01], [PKOBO-vote01], [Telop01], [Gallery01], [CalendarForm01], and [Link01] [Calendar01] free edition ver1.0.0, [Calendar02] free edition ver1.0.0, [PKOBO-News01] free edition ver1.0.3 and earlier, [PKOBO-vote01] free edition ver1.0.1 and earlier, [Telop01] free edition ver1.0.0,	N/A	A-TEL-TELO-200820/279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[Gallery01] free edition ver1.0.3 and earlier, [CalendarForm01] free edition ver1.0.3 and earlier, and [Link01] free edition ver1.0.0 allows remote attackers to bypass authentication and log in to the product with administrative privileges via unspecified vectors. **CVE ID : CVE-2020-5616**		
teradici					
pcoip_standard_agent					
Uncontrolled Search Path Element	11-Aug-20	4.4	The support bundler in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows versions prior to 20.04.1 and 20.07.0 does not use hard coded paths for certain Windows binaries, which allows an attacker to gain elevated privileges via execution of a malicious binary placed in the system path. **CVE ID : CVE-2020-13177**	N/A	A-TER-PCOI-200820/280
Insufficient Verification of Data Authenticity	11-Aug-20	4.6	A function in the Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior to version 20.04.1 does not properly validate the signature of an external binary, which could allow an attacker to gain elevated privileges via execution in the context of	N/A	A-TER-PCOI-200820/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the PCoIP Agent process. **CVE ID : CVE-2020-13178**		
Information Exposure	11-Aug-20	2.1	Broker Protocol messages in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior to 20.04.1 are not cleaned up in server memory, which may allow an attacker to read confidential information from a memory dump via forcing a crashing during the single sign-on procedure. **CVE ID : CVE-2020-13179**	N/A	A-TER-PCOI-200820/282
managament_console					
Improper Restriction of Rendered UI Layers or Frames	11-Aug-20	4.3	The web server in the Teradici Managament console versions 20.04 and 20.01.1 did not properly set the X-Frame-Options HTTP header, which could allow an attacker to trick a user into clicking a malicious link via clickjacking. **CVE ID : CVE-2020-13174**	N/A	A-TER-MANA-200820/283
cloud_access_connector					
Inclusion of Functionality from Untrusted Control Sphere	11-Aug-20	5	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 20, 2020 (v15 and earlier for Cloud Access Connector) contains a local file inclusion vulnerability which allows an	N/A	A-TER-CLOU-200820/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated remote attacker to leak LDAP credentials via a specially crafted HTTP request. **CVE ID : CVE-2020-13175**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-20	4.3	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 24, 2020 (v16 and earlier for the Cloud Access Connector) contains a stored cross-site scripting (XSS) vulnerability which allows a remote unauthenticated attacker to poison log files with malicious JavaScript via the login page which is executed when an administrator views the logs within the application. **CVE ID : CVE-2020-13176**	N/A	A-TER-CLOU-200820/285
cloud_access_connector_legacy					
Inclusion of Functionality from Untrusted Control Sphere	11-Aug-20	5	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 20, 2020 (v15 and earlier for Cloud Access Connector) contains a local file inclusion vulnerability which allows an unauthenticated remote attacker to leak LDAP credentials via a specially crafted HTTP request.	N/A	A-TER-CLOU-200820/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13175		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-Aug-20	4.3	The Management Interface of the Teradici Cloud Access Connector and Cloud Access Connector Legacy for releases prior to April 24, 2020 (v16 and earlier for the Cloud Access Connector) contains a stored cross-site scripting (XSS) vulnerability which allows a remote unauthenticated attacker to poison log files with malicious JavaScript via the login page which is executed when an administrator views the logs within the application. **CVE ID : CVE-2020-13176**	N/A	A-TER-CLOU-200820/287
graphics_agent					
Uncontrolled Search Path Element	11-Aug-20	4.4	The support bundler in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows versions prior to 20.04.1 and 20.07.0 does not use hard coded paths for certain Windows binaries, which allows an attacker to gain elevated privileges via execution of a malicious binary placed in the system path. **CVE ID : CVE-2020-13177**	N/A	A-TER-GRAP-200820/288
Insufficient Verification of Data Authenticity	11-Aug-20	4.6	A function in the Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior	N/A	A-TER-GRAP-200820/289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to version 20.04.1 does not properly validate the signature of an external binary, which could allow an attacker to gain elevated privileges via execution in the context of the PCoIP Agent process. **CVE ID : CVE-2020-13178**		
Information Exposure	11-Aug-20	2.1	Broker Protocol messages in Teradici PCoIP Standard Agent for Windows and Graphics Agent for Windows prior to 20.04.1 are not cleaned up in server memory, which may allow an attacker to read confidential information from a memory dump via forcing a crashing during the single sign-on procedure. **CVE ID : CVE-2020-13179**	N/A	A-TER-GRAP-200820/290
thedaylightstudio					
fuel_cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	13-Aug-20	7.5	FUEL CMS 1.4.7 allows SQL Injection via the col parameter to /pages/items, /permissions/items, or /navigation/items. **CVE ID : CVE-2020-17463**	https://github.com/daylightstudio/FUEL-CMS/releases/tag/1.4.8	A-THE-FUEL-200820/291
themeinprogress					
nova_lite					
Improper Neutralizatio	12-Aug-20	4.3	search.php in the Nova Lite theme before 1.3.9 for	https://themes.trac.word	A-THE-NOVA-200820/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			WordPress allows Reflected XSS. **CVE ID : CVE-2020-17362**	press.org/browser/nova-lite/1.3.9/readme.txt?rev=134076	
Tiki					
tiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-20	4.3	Tiki before 21.2 allows XSS because [\s\/"\'] is not properly considered in lib/core/TikiFilter/PreventXss.php. **CVE ID : CVE-2020-16131**	N/A	A-TIK-TIKI-200820/293
tiny					
tinymce					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	14-Aug-20	4.3	A cross-site scripting (XSS) vulnerability in TinyMCE 5.2.1 and earlier allows remote attackers to inject arbitrary web script when configured in classic editing mode. **CVE ID : CVE-2020-12648**	N/A	A-TIN-TINY-200820/294
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-Aug-20	4.3	TinyMCE before 4.9.7 and 5.x before 5.1.4 allows XSS in the core parser, the paste plugin, and the visualchars plugin by using the clipboard or APIs to insert content into the editor. **CVE ID : CVE-2020-17480**	N/A	A-TIN-TINY-200820/295
Trendmicro					
deep_security					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**	N/A	A-TRE-DEEP-200820/296
apex_one					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained	N/A	A-TRE-APEX-200820/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**		
officescan					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**	N/A	A-TRE-OFFI-200820/298
antivirus_toolkit					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an	N/A	A-TRE-ANTI-200820/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**		
officescan_business_security					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**	N/A	A-TRE-OFFI-200820/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
officescan_business_security_service					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**	N/A	A-TRE-OFFI-200820/301
officescan_cloud					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must	N/A	A-TRE-OFFI-200820/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**		
online_scan					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**	N/A	A-TRE-ONLI-200820/303
portable_security					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection	N/A	A-TRE-PORT-200820/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**		
rootkit_buster					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability.	N/A	A-TRE-ROOT-200820/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8607		
safe_lock					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**	N/A	A-TRE-SAFE-200820/306
serverprotect					
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel	N/A	A-TRE-SERV-200820/307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**		
turcom					
trcwifizone					
Improper Authenticati on	11-Aug-20	7.5	Turcom TRCwifiZone through 2020-08-10 allows authentication bypass by visiting manage/control.php and ignoring 302 Redirect responses. **CVE ID : CVE-2020-17466**	N/A	A-TUR-TRCW-200820/308
Usvn					
user-friendly_svn					
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	05-Aug-20	4.3	USVN (aka User-friendly SVN) before 1.0.9 allows XSS via SVN logs. **CVE ID : CVE-2020-17364**	N/A	A-USV-USER-200820/309
Vmware					
spring_cloud_netflix					
Externally Controlled Reference to a Resource in Another Sphere	07-Aug-20	4	Spring Cloud Netflix, versions 2.2.x prior to 2.2.4, versions 2.1.x prior to 2.1.6, and older unsupported versions allow applications to use the Hystrix Dashboard	https://tanzu.vmware.com/security/cve-2020-5412	A-VMW-SPRI-200820/310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			proxy.stream endpoint to make requests to any server reachable by the server hosting the dashboard. A malicious user, or attacker, can send a request to other servers that should not be exposed publicly. **CVE ID : CVE-2020-5412**		
X.org					
libx11					
Integer Overflow or Wraparound	05-Aug-20	4.6	An integer overflow leading to a heap-buffer overflow was found in The X Input Method (XIM) client was implemented in libX11 before version 1.6.10. As per upstream this is security relevant when setuid programs call XIM client functions while running with elevated privileges. No such programs are shipped with Red Hat Enterprise Linux. **CVE ID : CVE-2020-14344**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14344	A-X.O-LIBX-200820/311
xorg-server					
Improper Initialization	05-Aug-20	2.1	A flaw was found in the way xserver memory was not properly initialized. This could leak parts of server memory to the X client. In cases where Xorg server runs with elevated privileges, this could result in possible ASLR bypass. Xorg-server before version 1.20.9 is vulnerable.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14347	A-X.O-XORG-200820/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-14347		
Zohocorp					
manageengine_adselfservice_plus					
Improper Privilege Management	11-Aug-20	10	An elevation of privilege vulnerability exists in ManageEngine ADSelfService Plus before build 6003 because it does not properly enforce user privileges associated with a Certificate dialog. This vulnerability could allow an unauthenticated attacker to escalate privileges on a Windows host. An attacker does not require any privilege on the target system in order to exploit this vulnerability. One option is the self-service option on the Windows login screen. Upon selecting this option, the thick-client software is launched, which connects to a remote ADSelfService Plus server to facilitate self-service operations. An unauthenticated attacker having physical access to the host could trigger a security alert by supplying a self-signed SSL certificate to the client. The View Certificate option from the security alert allows an attacker to export a displayed certificate to a file. This can further cascade to a	https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6003-release-faceid-support	A-ZOH-MANA-200820/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dialog that can open Explorer as SYSTEM. By navigating from Explorer to \windows\system32, cmd.exe can be launched as a SYSTEM. **CVE ID : CVE-2020-11552**		
Operating System					
Apple					
iphone_os					
Improper Input Validation	10-Aug-20	4.3	A unicode RTL order character in the downloaded file name can be used to change the file's name during the download UI flow to change the file extension. This vulnerability affects Firefox for iOS < 28. **CVE ID : CVE-2020-15651**	N/A	O-APP-IPHO-200820/314
Canonical					
ubuntu_linux					
Missing Release of Resource after Effective Lifetime	06-Aug-20	2.1	In whoopsie, parse_report() from whoopsie.c allows a local attacker to cause a denial of service via a crafted file. The DoS is caused by resource exhaustion due to a memory leak. Fixed in 0.2.52.5ubuntu0.5, 0.2.62ubuntu0.5 and 0.2.69ubuntu0.1. **CVE ID : CVE-2020-11937**	https://github.com/sungjungk/whoopsie_killer, https://launchpad.net/bugs/1881982, https://usn.ubuntu.com/4450-1	O-CAN-UBUN-200820/315
Improper Handling of Exceptional	06-Aug-20	2.1	An unhandled exception in check_ignored() in apport/report.py can be exploited by a local	https://launchpad.net/bugs/1877023,	O-CAN-UBUN-200820/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			attacker to cause a denial of service. If the mtime attribute is a string value in apport-ignore.xml, it will trigger an unhandled exception, resulting in a crash. Fixed in 2.20.1-0ubuntu2.24, 2.20.9-0ubuntu7.16, 2.20.11-0ubuntu27.6. **CVE ID : CVE-2020-15701**	https://usn.ubuntu.com/4449-1	
Time-of-check Time-of-use (TOCTOU) Race Condition	06-Aug-20	4.4	TOCTOU Race Condition vulnerability in apport allows a local attacker to escalate privileges and execute arbitrary code. An attacker may exit the crashed process and exploit PID recycling to spawn a root process with the same PID as the crashed process, which can then be used to escalate privileges. Fixed in 2.20.1-0ubuntu2.24, 2.20.9 versions prior to 2.20.9-0ubuntu7.16 and 2.20.11 versions prior to 2.20.11-0ubuntu27.6. Was ZDI-CAN-11234. **CVE ID : CVE-2020-15702**	https://usn.ubuntu.com/4449-1	O-CAN-UBUN-200820/317
cayintech					
cms-se_firmware					
Improper Neutralization of Special Elements used in an OS Command	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and	N/A	O-CAY-CMS--200820/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**		
cms-se-lxc_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**	N/A	O-CAY-CMS--200820/319
cms-60_firmware					
Improper Neutralization of Special Elements used in an OS	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be	N/A	O-CAY-CMS--200820/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**		
cms-40_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**	N/A	O-CAY-CMS--200820/321
cms-20_firmware					
Improper Neutralization of Special Elements	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default	N/A	O-CAY-CMS--200820/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**		
cms					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**	N/A	O-CAY-CMS-200820/323
Debian					
debian_linux					
Improper Limitation of	03-Aug-20	6.8	In kerfuffle/jobs.cpp in KDE Ark before 20.08.0, a	https://invent.kde.org/ut	O-DEB-DEBI-200820/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			crafted archive can install files outside the extraction directory via ../ directory traversal. **CVE ID : CVE-2020-16116**	ilities/ark/-/commit/0df592524fed305d6fbe74ddf8a196bc9ffdb92f, https://kde.org/info/security/advisory-20200730-1.txt, https://www.debian.org/security/2020/dsa-4738	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Aug-20	4.6	Firejail through 0.9.62 does not honor the -- end-of-options indicator after the --output option, which may lead to command injection. **CVE ID : CVE-2020-17367**	N/A	O-DEB-DEBI-200820/325
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	11-Aug-20	7.5	Firejail through 0.9.62 mishandles shell metacharacters during use of the --output or --output-stderr option, which may lead to command injection. **CVE ID : CVE-2020-17368**	N/A	O-DEB-DEBI-200820/326
digitus					
da-70254_firmware					
Insufficiently Protected Credentials	07-Aug-20	3.3	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to elevate	N/A	O-DIG-DA-7-200820/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic. **CVE ID : CVE-2020-15062**		
Improper Authentication	07-Aug-20	8.3	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter. **CVE ID : CVE-2020-15063**	N/A	O-DIG-DA-7-200820/328
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-20	2.3	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name. **CVE ID : CVE-2020-15064**	N/A	O-DIG-DA-7-200820/329
Improper Input Validation	07-Aug-20	6.1	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to denial-of-service the device via long input values. **CVE ID : CVE-2020-15065**	N/A	O-DIG-DA-7-200820/330
fanuc					
series_30i_firmware					
Improper Input	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i	N/A	O-FAN-SERI-200820/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**		
series_31i_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/332
series_32i-b_plus_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/333
series_35i-b_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become	N/A	O-FAN-SERI-200820/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inaccessible to other devices. **CVE ID : CVE-2020-12739**		
power_motion_i-model_a_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-POWE-200820/335
series_0i-model_f_plus_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/336
series_0i-model_f_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/337
series_32i-model_a_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/338
series_0i-model_d_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/339
series_0i-mate_d_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/340
series_0i-model_c_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote	N/A	O-FAN-SERI-200820/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**		
series_16i_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/342
series_18i_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/343
series_21i-model_b_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
series_0i-model_b_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/345
series_18i-wb_firmware					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	O-FAN-SERI-200820/346
Freebsd					
freebsd					
Improper Input Validation	06-Aug-20	4.6	In FreeBSD 12.1-STABLE before r362166, 12.1-RELEASE before p8, 11.4-STABLE before r362167, 11.4-RELEASE before p2, and 11.3-RELEASE before p12, missing length validation code common to mulitple USB network drivers allows a malicious USB device to write beyond the end of an allocated network packet buffer.	N/A	O-FRE-FREE-200820/347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7459		
Time-of-check Time-of-use (TOCTOU) Race Condition	06-Aug-20	4.4	In FreeBSD 12.1-STABLE before r363918, 12.1-RELEASE before p8, 11.4-STABLE before r363919, 11.4-RELEASE before p2, and 11.3-RELEASE before p12, the sendmsg system call in the compat32 subsystem on 64-bit platforms has a time-of-check to time-of-use vulnerability allowing a mailcious userspace program to modify control message headers after they were validation. **CVE ID : CVE-2020-7460**	N/A	O-FRE-FREE-200820/348
Google					
android					
Time-of-check Time-of-use (TOCTOU) Race Condition	11-Aug-20	6.9	In updatePreferenceIntents of AccountTypePreferenceLoader, there is a possible confused deputy attack due to a race condition. This could lead to local escalation of privilege and launching privileged activities with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-150946634	N/A	O-GOO-ANDR-200820/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0238		
Information Exposure	11-Aug-20	4.9	In getDocumentMetadata of DocumentsContract.java, there is a possible disclosure of location metadata from a file due to a permissions bypass. This could lead to local information disclosure from a file (eg. a photo) containing location metadata with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-151095863 **CVE ID : CVE-2020-0239**	N/A	O-GOO-ANDR-200820/350
Out-of-bounds Write	11-Aug-20	9.3	In NewFixedDoubleArray of factory.cc, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150706594 **CVE ID : CVE-2020-0240**	N/A	O-GOO-ANDR-200820/351
Double Free	11-Aug-20	7.2	In NuPlayerStreamListener of NuPlayerStreamListener.c	N/A	O-GOO-ANDR-200820/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pp, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-151456667 **CVE ID : CVE-2020-0241**		
Use After Free	11-Aug-20	7.2	In reset of NuPlayerDriver.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the media server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-151643722 **CVE ID : CVE-2020-0242**	N/A	O-GOO-ANDR-200820/353
Use After Free	11-Aug-20	7.2	In clearPropValue of MediaAnalyticsItem.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the media server with no additional execution privileges needed. User interaction is not needed	N/A	O-GOO-ANDR-200820/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-8.0 Android-8.1Android ID: A-151644303 **CVE ID : CVE-2020-0243**		
Loop with Unreachable Exit Condition ('Infinite Loop')	11-Aug-20	4.9	In Threshold::getHistogram of ImageProcessHelper.java, there is a possible crash loop due to an uncaught exception. This could lead to local denial of service with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-8.0 Android-8.1Android ID: A-156087409 **CVE ID : CVE-2020-0247**	N/A	O-GOO-ANDR-200820/355
Information Exposure	11-Aug-20	4.9	In postInstantAppNotif of InstantAppNotifier.java, there is a possible permission bypass due to a PendingIntent error. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-154627439 **CVE ID : CVE-2020-0248**	N/A	O-GOO-ANDR-200820/356
Information	11-Aug-20	4.9	In postInstantAppNotif of	N/A	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			InstantAppNotifier.java, there is a possible permission bypass due to a PendingIntent error. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.0 Android-8.1 Android-9Android ID: A-154719656 **CVE ID : CVE-2020-0249**		ANDR-200820/357
Information Exposure	11-Aug-20	4.9	In requestCellInfoUpdateInternal of PhoneInterfaceManager.java, there is a missing permission check. This could lead to local information disclosure of location data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-154934934 **CVE ID : CVE-2020-0250**	N/A	O-GOO-ANDR-200820/358
Out-of-bounds Read	11-Aug-20	7.8	There is a possible out of bounds read due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-152647626	N/A	O-GOO-ANDR-200820/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0251		
Use After Free	11-Aug-20	10	There is a possible memory corruption due to a use after free.Product: AndroidVersions: Android SoCAndroid ID: A-152236803 **CVE ID : CVE-2020-0252**	N/A	O-GOO-ANDR-200820/360
Use After Free	11-Aug-20	10	There is a possible memory corruption due to a use after free.Product: AndroidVersions: Android SoCAndroid ID: A-152647365 **CVE ID : CVE-2020-0253**	N/A	O-GOO-ANDR-200820/361
Improper Privilege Management	11-Aug-20	7.2	In postNotification of ServiceRecord.java, there is a possible bypass of foreground process restrictions due to an uncaught exception. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-140108616 **CVE ID : CVE-2020-0108**	N/A	O-GOO-ANDR-200820/362
Out-of-bounds Read	11-Aug-20	7.8	There is a possible out of bounds read due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-152647751	N/A	O-GOO-ANDR-200820/363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0254		
Out-of-bounds Write	11-Aug-20	7.2	In LoadPartitionTable of gpt.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege when inserting a malicious USB device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-8.0Android ID: A-152874864 **CVE ID : CVE-2020-0256**	N/A	O-GOO-ANDR-200820/364
Improper Privilege Management	11-Aug-20	7.2	In SpecializeCommon of com_android_internal_os_Zygote.cpp, there is a permissions bypass due to an incomplete cleanup. This could lead to local escalation of privilege in isolated processes with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-156741968 **CVE ID : CVE-2020-0257**	N/A	O-GOO-ANDR-200820/365
Information Exposure	11-Aug-20	4.9	In stopZygoteLocked of AppZygote.java, there is an insufficient cleanup. This could lead to local information disclosure in the application that is	N/A	O-GOO-ANDR-200820/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			started next with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-157598956 **CVE ID : CVE-2020-0258**		
Improper Privilege Management	11-Aug-20	7.2	In android_verity_ctr of dm-android-verity.c, there is a possible way to modify a dm-verity protected filesystem due to improperly used crypto. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-157941353References: N/A **CVE ID : CVE-2020-0259**	N/A	O-GOO-ANDR-200820/367
Out-of-bounds Read	11-Aug-20	6.4	There is a possible out of bounds read due to an incorrect bounds check.Product: AndroidVersions: Android SoCAndroid ID: A-152225183 **CVE ID : CVE-2020-0260**	N/A	O-GOO-ANDR-200820/368
Information Exposure	10-Aug-20	5	A Content Provider in Firefox for Android allowed local files accessible by the browser to be read by a remote	N/A	O-GOO-ANDR-200820/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			webpage, leading to sensitive data disclosure, including cookies for other origins. This vulnerability affects Firefox for < Android. **CVE ID : CVE-2020-15647**		
Unrestricted Upload of File with Dangerous Type	10-Aug-20	4.3	Given an installed malicious file picker application, an attacker was able to steal and upload local files of their choosing, regardless of the actually files picked. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.11. **CVE ID : CVE-2020-15649**	N/A	O-GOO-ANDR-200820/370
N/A	10-Aug-20	4.3	Given an installed malicious file picker application, an attacker was able to overwrite local files and thus overwrite Firefox settings (but not access the previous profile). *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 68.11. **CVE ID : CVE-2020-15650**	N/A	O-GOO-ANDR-200820/371
Huawei					
honor_20_firmware					
Improper Authenticati	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than	N/A	O-HUA-HONO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication		200820/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
honor_20_pro_firmware					
Improper Authenticati on	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P1 1);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P 8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions	N/A	O-HUA-HONO-200820/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
honor_v20_firmware					
Improper Authenticati on	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than	N/A	O-HUA-HONO-200820/374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
mate_20_pro_firmware					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro	N/A	O-HUA-MATE-200820/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
p30_pro_firmware					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11)	N/A	O-HUA-P30_-200820/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
Incorrect Authorization	10-Aug-20	4.3	HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) have a denial of service vulnerability. Certain system configuration can be modified because of improper authorization. The attacker could trick the user installing and executing a malicious application, successful exploit could cause a denial of service condition of PHONE function. **CVE ID : CVE-2020-9245**	N/A	O-HUA-P30_-200820/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
p30_firmware					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions Versions earlier than	N/A	O-HUA-P30_-200820/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
Incorrect Authorization	10-Aug-20	4.3	HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) have a denial of service vulnerability. Certain system configuration can be modified because of improper authorization. The attacker could trick the user installing and executing a malicious application, successful exploit could cause a denial of service condition of PHONE function. **CVE ID : CVE-2020-9245**	N/A	O-HUA-P30_-200820/379
mate_20_x_firmware					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5),	N/A	O-HUA-MATE-200820/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
mate_20_firmware					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12)	N/A	O-HUA-MATE-200820/381

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
honor_magic_2_firmware					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8)	N/A	O-HUA-HONO-200820/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
mate_20_rs_firmware					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5),	N/A	O-HUA-MATE-200820/383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			forged **CVE ID : CVE-2020-9244**		
mate_30_firmware					
Uncontrolled Recursion	10-Aug-20	4.3	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a denial of service vulnerability. The system does not properly limit the depth of recursion, an attacker should trick the user installing and execute a malicious application. Successful exploit could cause a denial of service condition. **CVE ID : CVE-2020-9243**	N/A	O-HUA-MATE-200820/384
lindy-international					
42633_firmware					
Insufficiently Protected Credentials	07-Aug-20	3.3	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic. **CVE ID : CVE-2020-15058**	N/A	O-LIN-4263-200820/385
Improper Authenticati on	07-Aug-20	8.3	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password	N/A	O-LIN-4263-200820/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter. **CVE ID : CVE-2020-15059**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-20	2.3	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name. **CVE ID : CVE-2020-15060**	N/A	O-LIN-4263-200820/387
Improper Input Validation	07-Aug-20	6.1	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to denial-of-service the device via long input values. **CVE ID : CVE-2020-15061**	N/A	O-LIN-4263-200820/388
Linux					
linux_kernel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-20	4.3	A GET-based XSS reflected vulnerability in Plesk Onyx 17.8.11 allows remote unauthenticated users to inject arbitrary JavaScript, HTML, or CSS via a GET parameter. **CVE ID : CVE-2020-11584**	N/A	O-LIN-LINU-200820/389
Microsoft					
windows					
Download of Code Without Integrity Check	06-Aug-20	4.6	MyBrowserPlus downloads the files needed to run the program through the setup file (Setup.inf). At this time,	N/A	O-MIC-WIND-200820/390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			there is a vulnerability in downloading arbitrary files due to insufficient integrity verification of the files. **CVE ID : CVE-2020-7817**		
Out-of-bounds Write	04-Aug-20	6.8	DaviewIndy has a Heap-based overflow vulnerability, triggered when the user opens a malformed image file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7822**	N/A	O-MIC-WIND-200820/391
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-Aug-20	4.3	A GET-based XSS reflected vulnerability in Plesk Obsidian 18.0.17 allows remote unauthenticated users to inject arbitrary JavaScript, HTML, or CSS via a GET parameter. **CVE ID : CVE-2020-11583**	N/A	O-MIC-WIND-200820/392
Uncontrolled Search Path Element	10-Aug-20	6.9	Firefox could be made to load attacker-supplied DLL files from the installation directory. This required an attacker that is already capable of placing files in the installation directory. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird <	N/A	O-MIC-WIND-200820/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			78.1. **CVE ID : CVE-2020-15657**		
Incorrect Permission Assignment for Critical Resource	04-Aug-20	1.9	IBM Spectrum Protect Plus 10.1.0 through 10.1.6 agent files, in non-default configurations, on Windows are assigned access to everyone with full control permissions, which could allow a local user to cause interruption of the service operations. IBM X-Force ID: 185372. **CVE ID : CVE-2020-4631**	https://www.ibm.com/support/pages/node/6255116	O-MIC-WIND-200820/394
Improper Validation of Integrity Check Value	07-Aug-20	6.8	hslogin2.dll ActiveX Control in Groupware contains a vulnerability that could allow remote files to be downloaded and executed by setting the arguments to the activex method. This is due to a lack of integrity verification of the policy files referenced in the update process, and a remote attacker could induce a user to crafted web page, causing damage such as malicious code infection. **CVE ID : CVE-2020-7810**	N/A	O-MIC-WIND-200820/395
Improper Input Validation	05-Aug-20	7.2	An input validation vulnerability found in multiple Trend Micro products utilizing a particular version of a specific rootkit protection driver could allow an	N/A	O-MIC-WIND-200820/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker in user-mode with administrator permissions to abuse the driver to modify a kernel address that may cause a system crash or potentially lead to code execution in kernel mode. An attacker must already have obtained administrator access on the target machine (either legitimately or via a separate unrelated attack) to exploit this vulnerability. **CVE ID : CVE-2020-8607**		
opengroup					
unix					
Missing Authentication for Critical Function	12-Aug-20	6.4	Xvfb of SAP Business Objects Business Intelligence Platform, versions - 4.2, 4.3, platform on Unix does not perform any authentication checks for functionalities that require user identity. **CVE ID : CVE-2020-6294**	N/A	O-OPE-UNIX-200820/397
Opensuse					
leap					
Access of Resource Using Incompatible Type ('Type Confusion')	10-Aug-20	9.3	JIT optimizations involving the Javascript arguments object could confuse later optimizations. This risk was already mitigated by various precautions in the code, resulting in this bug rated at only moderate severity. This vulnerability	N/A	O-OPE-LEAP-200820/398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1. **CVE ID : CVE-2020-15656**		
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Aug-20	5	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary via invalid inputs. **CVE ID : CVE-2020-16845**	https://groups.google.com/forum/#!topic/golang-announce/NyPIaucMgXo	O-OPE-LEAP-200820/399
Incorrect Default Permissions	07-Aug-20	7.2	A Incorrect Default Permissions vulnerability in the packaging of inn in openSUSE Leap 15.2, openSUSE Tumbleweed, openSUSE Leap 15.1 allows local attackers with control of the new user to escalate their privileges to root. This issue affects: openSUSE Leap 15.2 inn version 2.6.2-lp152.1.26 and prior versions. openSUSE Tumbleweed inn version 2.6.2-4.2 and prior versions. openSUSE Leap 15.1 inn version 2.5.4-lp151.3.3.1 and prior versions. **CVE ID : CVE-2020-8026**	https://bugzilla.suse.com/show_bug.cgi?id=1172573	O-OPE-LEAP-200820/400
robotemi					
launcher_os					
Missing Authentication for Critical	07-Aug-20	6.4	Missing Authentication for Critical Function in Robotemi Global Ltd Temi Firmware up to 20190419.165201,	N/A	O-ROB-LAUN-200820/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			Launcher OS prior to 11969-13146, Robox OS prior to 117.21-119.24, and their Android phone app prior to 1.3.3-1.3.7931 allows remote attackers to receive and answer calls intended for another temi user. Answering the call this way grants motor control of the temi in addition to audio/video. **CVE ID : CVE-2020-16167**		
temi_firmware					
Origin Validation Error	07-Aug-20	4.3	Origin Validation Error in Robotemi Global Ltd Temi Firmware up to 20190419.165201, Launcher OS prior to 11969-13146, Robox OS prior to 117.21-119.24, and their Android phone app prior to 1.3.3-1.3.7931 allows remote attackers to access the custom API server and MQTT broker used by the temi and send it custom data/requests. **CVE ID : CVE-2020-16168**	N/A	O-ROB-TEMI-200820/402
robox_os					
Improper Authentication	07-Aug-20	7.5	Authentication Bypass Using an Alternate Path or Channel in Robotemi Global Ltd Temi Firmware up to 20190419.165201, Launcher OS prior to 11969-13146, Robox OS prior to 117.21-119.24, and their Android phone	N/A	O-ROB-ROBO-200820/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			app prior to 1.3.3-1.3.7931 allows remote attackers to listen in on any ongoing calls between temi robots and their users if they can brute-force/guess a six-digit value. **CVE ID : CVE-2020-16169**		
Sophos					
xg_firewall_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	07-Aug-20	6.5	Two OS command injection vulnerabilities in the User Portal of Sophos XG Firewall through 2020-08-05 potentially allow an authenticated attacker to remotely execute arbitrary code. **CVE ID : CVE-2020-17352**	N/A	O-SOP-XG_F-200820/404
Suse					
linux_enterprise_server					
Incorrect Execution-Assigned Permissions	07-Aug-20	4.6	A Incorrect Execution-Assigned Permissions vulnerability in the permissions package of SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1, openSUSE Tumbleweed sets the permissions for some of the directories of the pcp package to unintended settings. This issue affects: SUSE Linux Enterprise Server 12-SP4 permissions versions prior	https://bugzilla.suse.com/show_bug.cgi?id=1171883	O-SUS-LINU-200820/405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 20170707-3.24.1. SUSE Linux Enterprise Server 15-LTSS permissions versions prior to 20180125-3.27.1. SUSE Linux Enterprise Server for SAP 15 permissions versions prior to 20180125-3.27.1. openSUSE Leap 15.1 permissions versions prior to 20181116-lp151.4.24.1. openSUSE Tumbleweed permissions versions prior to 20200624. **CVE ID : CVE-2020-8025**		
linux_enterprise_software_development_kit					
Incorrect Execution-Assigned Permissions	07-Aug-20	4.6	A Incorrect Execution-Assigned Permissions vulnerability in the permissions package of SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1, openSUSE Tumbleweed sets the permissions for some of the directories of the pcp package to unintended settings. This issue affects: SUSE Linux Enterprise Server 12-SP4 permissions versions prior to 20170707-3.24.1. SUSE Linux Enterprise Server 15-LTSS permissions versions prior to 20180125-3.27.1. SUSE	https://bugzilla.suse.com/show_bug.cgi?id=1171883	O-SUS-LINU-200820/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Linux Enterprise Server for SAP 15 permissions versions prior to 20180125-3.27.1. openSUSE Leap 15.1 permissions versions prior to 20181116-lp151.4.24.1. openSUSE Tumbleweed permissions versions prior to 20200624. **CVE ID : CVE-2020-8025**		
linux_enterprise_high_performance_computing					
Incorrect Execution-Assigned Permissions	07-Aug-20	4.6	A Incorrect Execution-Assigned Permissions vulnerability in the permissions package of SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15; openSUSE Leap 15.1, openSUSE Tumbleweed sets the permissions for some of the directories of the pcp package to unintended settings. This issue affects: SUSE Linux Enterprise Server 12-SP4 permissions versions prior to 20170707-3.24.1. SUSE Linux Enterprise Server 15-LTSS permissions versions prior to 20180125-3.27.1. SUSE Linux Enterprise Server for SAP 15 permissions versions prior to 20180125-3.27.1. openSUSE Leap 15.1	https://bugzilla.suse.com/show_bug.cgi?id=1171883	O-SUS-LINU-200820/407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions versions prior to 20181116-lp151.4.24.1. openSUSE Tumbleweed permissions versions prior to 20200624. **CVE ID : CVE-2020-8025**		
Swisscom					
internet_box_2_firmware					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**	N/A	O-SWI-INTE-200820/408
internet_box_standard_firmware					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials	N/A	O-SWI-INTE-200820/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**		
internet_box_plus_firmware					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**	N/A	O-SWI-INTE-200820/410
internet_box_3_firmware					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to	N/A	O-SWI-INTE-200820/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**		
internet_box_light_firmware					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**	N/A	O-SWI-INTE-200820/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
teltonika-networks					
trb245_firmware					
Cross-Site Request Forgery (CSRF)	03-Aug-20	6.8	Cross-site request forgery in Teltonika firmware TRB2_R_00.02.04.01 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link. **CVE ID : CVE-2020-5770**	N/A	O-TEL-TRB2-200820/413
Unrestricted Upload of File with Dangerous Type	03-Aug-20	9	Improper Input Validation in Teltonika firmware TRB2_R_00.02.04.01 allows a remote, authenticated attacker to gain root privileges by uploading a malicious backup archive. **CVE ID : CVE-2020-5771**	N/A	O-TEL-TRB2-200820/414
Unrestricted Upload of File with Dangerous Type	03-Aug-20	9	Improper Input Validation in Teltonika firmware TRB2_R_00.02.04.01 allows a remote, authenticated attacker to gain root privileges by uploading a malicious package file. **CVE ID : CVE-2020-5772**	N/A	O-TEL-TRB2-200820/415
Improper Privilege Management	03-Aug-20	6.5	Improper Access Control in Teltonika firmware TRB2_R_00.02.04.01 allows a low privileged user to perform unauthorized write operations. **CVE ID : CVE-2020-5773**	N/A	O-TEL-TRB2-200820/416
Tp-link					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tl-ps310u_firmware					
Insufficiently Protected Credentials	07-Aug-20	3.3	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic. **CVE ID : CVE-2020-15054**	N/A	O-TP--TL-P-200820/417
Improper Authenticati on	07-Aug-20	8.3	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter. **CVE ID : CVE-2020-15055**	N/A	O-TP--TL-P-200820/418
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-20	2.3	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name. **CVE ID : CVE-2020-15056**	N/A	O-TP--TL-P-200820/419
Improper Input Validation	07-Aug-20	6.1	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to denial-of-service the device via long input values.	N/A	O-TP--TL-P-200820/420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15057		
Yokogawa					
centum_cs_3000_firmware					
Improper Authenticati on	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**	N/A	O-YOK-CENT-200820/421
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **CVE ID : CVE-2020-5609**	N/A	O-YOK-CENT-200820/422
centum_vp_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**	N/A	O-YOK-CENT-200820/423
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **CVE ID : CVE-2020-5609**	N/A	O-YOK-CENT-200820/424
b\/m9000cs_firmware					
Improper Authentication	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP	N/A	O-YOK-B\/M-200820/425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **CVE ID : CVE-2020-5609**	N/A	O-YOK-B\/M-200820/426
b\/m9000vp_firmware					
Improper Authenticati on	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote	N/A	O-YOK-B\/M-200820/427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **CVE ID : CVE-2020-5609**	N/A	O-YOK-B\/M-200820/428
zyzel					
nas326_firmware					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310	N/A	O-ZYZ-NAS3-200820/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**		
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0;	N/A	O-ZYZ-NAS3-200820/430

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**		
nas520_firmware					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**	N/A	O-ZYZ-NAS5-200820/431
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a	N/A	O-ZYZ-NAS5-200820/432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**		
nas540_firmware					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and	N/A	O-ZYZ-NAS5-200820/433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**		
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and	N/A	O-ZYZ-NAS5-200820/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**		
nas542_firmware					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**	N/A	O-ZYZ-NAS5-200820/435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**	N/A	O-ZYZ-NAS5-200820/436
Hardware					
cayintech					
cms-se					
Improper Neutralization of Special Elements	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default	N/A	H-CAY-CMS--200820/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**		
cms-se-lxc					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**	N/A	H-CAY-CMS--200820/438
cms-60					
Improper Neutralization of Special	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection	N/A	H-CAY-CMS--200820/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**		
cms-40					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**	N/A	H-CAY-CMS--200820/440
cms-20					
Improper Neutralizatio	06-Aug-20	9	Cayin CMS suffers from an authenticated OS semi-	N/A	H-CAY-CMS--200820/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			blind command injection vulnerability using default credentials. This can be exploited to inject and execute arbitrary shell commands as the root user through the 'NTP_Server_IP' HTTP POST parameter in system.cgi page. This issue affects several branches and versions of the CMS application, including CME-SE, CMS-60, CMS-40, CMS-20, and CMS version 8.2, 8.0, and 7.5. **CVE ID : CVE-2020-7357**		
digitus					
da-70254					
Insufficiently Protected Credentials	07-Aug-20	3.3	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic. **CVE ID : CVE-2020-15062**	N/A	H-DIG-DA-7-200820/442
Improper Authenticati on	07-Aug-20	8.3	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter.	N/A	H-DIG-DA-7-200820/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15063		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-20	2.3	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name. **CVE ID : CVE-2020-15064**	N/A	H-DIG-DA-7-200820/444
Improper Input Validation	07-Aug-20	6.1	DIGITUS DA-70254 4-Port Gigabit Network Hub 2.073.000.E0008 devices allow an attacker on the same network to denial-of-service the device via long input values. **CVE ID : CVE-2020-15065**	N/A	H-DIG-DA-7-200820/445
fanuc					
series_30i					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/446
series_31i					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an	N/A	H-FAN-SERI-200820/447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**		
series_32i-b_plus					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/448
series_35i-b					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/449
power_motion_i-model_a					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-POWE-200820/450

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
series_0i-model_f_plus					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/451
series_0i-model_f					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/452
series_32i-model_a					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/453
series_0i-model_d					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an	N/A	H-FAN-SERI-200820/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**		
series_0i-mate_d					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/455
series_0i-model_c					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/456
series_16i					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices.	N/A	H-FAN-SERI-200820/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12739		
series_18i					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/458
series_21i-model_b					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/459
series_0i-model_b					
Improper Input Validation	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**	N/A	H-FAN-SERI-200820/460
series_18i-wb					
Improper Input	03-Aug-20	5	A denial-of-service vulnerability in the Fanuc i Series CNC (0i-MD and 0i	N/A	H-FAN-SERI-200820/461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Mate-MD) could allow an unauthenticated, remote attacker to cause an affected CNC to become inaccessible to other devices. **CVE ID : CVE-2020-12739**		
Huawei					
honor_20					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than	N/A	H-HUA-HONO-200820/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
honor_20_pro					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P1	N/A	H-HUA-HONO-200820/463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
honor_v20					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier	N/A	H-HUA-HONO-200820/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
mate_20_pro					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions	N/A	H-HUA-MATE-200820/465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
p30_pro					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier	N/A	H-HUA-P30_-200820/466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P 8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
Incorrect Authorizatio n	10-Aug-20	4.3	HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P1 1);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) have a denial of service vulnerability. Certain	N/A	H-HUA-P30_- 200820/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system configuration can be modified because of improper authorization. The attacker could trick the user installing and executing a malicious application, successful exploit could cause a denial of service condition of PHONE function. **CVE ID : CVE-2020-9245**		
p30					
Improper Authenticati on	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P1 1);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P 8);HonorMagic2 versions Versions earlier than	N/A	H-HUA-P30-200820/468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
Incorrect Authorization	10-Aug-20	4.3	HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) have a denial of service vulnerability. Certain system configuration can be modified because of improper authorization. The attacker could trick the user installing and executing a malicious application, successful exploit could cause a	N/A	H-HUA-P30-200820/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			denial of service condition of PHONE function. **CVE ID : CVE-2020-9245**		
mate_20_x					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions	N/A	H-HUA-MATE-200820/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
mate_20					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) ;HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS	N/A	H-HUA-MATE-200820/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
honor_magic_2					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than	N/A	H-HUA-HONO-200820/472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8) ;HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11) ;Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12) ;HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11) ;HonorV20 versions Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9244		
mate_20_rs					
Improper Authentication	11-Aug-20	4.6	HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8);HUAWEI Mate 20 Pro versions Versions earlier than 10.1.0.270(C431E7R1P5), Versions earlier than 10.1.0.270(C635E3R1P5), Versions earlier than 10.1.0.273(C636E7R2P4); HUAWEI Mate 20 X versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11);HUAWEI P30 Pro versions Versions earlier than 10.1.0.160(C00E160R2P8);HUAWEI Mate 20 RS versions Versions earlier than 10.1.0.160(C786E160R3P8);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);Honor20 versions Versions earlier than 10.0.0.175(C00E58R4P11);Honor20 PRO versions Versions earlier than 10.0.0.194(C00E62R8P12);HonorMagic2 versions Versions earlier than 10.0.0.187(C00E61R2P11);HonorV20 versions	N/A	H-HUA-MATE-200820/473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Versions earlier than 10.0.0.188(C00E62R2P11) have an improper authentication vulnerability. The system does not properly sign certain encrypted file, the attacker should gain the key used to encrypt the file, successful exploit could cause certain file be forged **CVE ID : CVE-2020-9244**		
mate_30					
Uncontrolled Recursion	10-Aug-20	4.3	HUAWEI Mate 30 with versions earlier than 10.1.0.150(C00E136R5P3) have a denial of service vulnerability. The system does not properly limit the depth of recursion, an attacker should trick the user installing and execute a malicious application. Successful exploit could cause a denial of service condition. **CVE ID : CVE-2020-9243**	N/A	H-HUA-MATE-200820/474
lindy-international					
42633					
Insufficiently Protected Credentials	07-Aug-20	3.3	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP	N/A	H-LIN-4263-200820/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic. **CVE ID : CVE-2020-15058**		
Improper Authentication	07-Aug-20	8.3	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter. **CVE ID : CVE-2020-15059**	N/A	H-LIN-4263-200820/476
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-20	2.3	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name. **CVE ID : CVE-2020-15060**	N/A	H-LIN-4263-200820/477
Improper Input Validation	07-Aug-20	6.1	Lindy 42633 4-Port USB 2.0 Gigabit Network Server 2.078.000 devices allow an attacker on the same network to denial-of-service the device via long input values. **CVE ID : CVE-2020-15061**	N/A	H-LIN-4263-200820/478
robotemi					
temi					
Origin Validation Error	07-Aug-20	4.3	Origin Validation Error in Robotemi Global Ltd Temi Firmware up to 20190419.165201, Launcher OS prior to 11969-13146, Robox OS	N/A	H-ROB-TEMI-200820/479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 117.21-119.24, and their Android phone app prior to 1.3.3-1.3.7931 allows remote attackers to access the custom API server and MQTT broker used by the temi and send it custom data/requests. **CVE ID : CVE-2020-16168**		
Swisscom					
internet_box_2					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**	N/A	H-SWI-INTE-200820/480
internet_box_standard					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and	N/A	H-SWI-INTE-200820/481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**		
internet_box_plus					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**	N/A	H-SWI-INTE-200820/482
internet_box_3					
Insufficiently	04-Aug-20	7.7	An issue was discovered	N/A	H-SWI-INTE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Protected Credentials			on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the superuser. **CVE ID : CVE-2020-16134**		200820/483
internet_box_light					
Insufficiently Protected Credentials	04-Aug-20	7.7	An issue was discovered on Swisscom Internet Box 2, Internet Box Standard, Internet Box Plus prior to 10.04.38, Internet Box 3 prior to 11.01.20, and Internet Box light prior to 08.06.06. Given the (user-configurable) credentials for the local Web interface or physical access to a device's plus or reset button, an attacker can create a user with elevated privileges on the Sysbus-API. This can then be used to modify local or remote SSH access, thus allowing a login session as the	N/A	H-SWI-INTE-200820/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			superuser. **CVE ID : CVE-2020-16134**		
teltonika-networks					
trb245					
Cross-Site Request Forgery (CSRF)	03-Aug-20	6.8	Cross-site request forgery in Teltonika firmware TRB2_R_00.02.04.01 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link. **CVE ID : CVE-2020-5770**	N/A	H-TEL-TRB2-200820/485
Unrestricted Upload of File with Dangerous Type	03-Aug-20	9	Improper Input Validation in Teltonika firmware TRB2_R_00.02.04.01 allows a remote, authenticated attacker to gain root privileges by uploading a malicious backup archive. **CVE ID : CVE-2020-5771**	N/A	H-TEL-TRB2-200820/486
Unrestricted Upload of File with Dangerous Type	03-Aug-20	9	Improper Input Validation in Teltonika firmware TRB2_R_00.02.04.01 allows a remote, authenticated attacker to gain root privileges by uploading a malicious package file. **CVE ID : CVE-2020-5772**	N/A	H-TEL-TRB2-200820/487
Improper Privilege Management	03-Aug-20	6.5	Improper Access Control in Teltonika firmware TRB2_R_00.02.04.01 allows a low privileged user to perform unauthorized write operations.	N/A	H-TEL-TRB2-200820/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5773		
Tp-link					
tl-ps310u					
Insufficiently Protected Credentials	07-Aug-20	3.3	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to elevate privileges because the administrative password can be discovered by sniffing unencrypted UDP traffic. **CVE ID : CVE-2020-15054**	N/A	H-TP--TL-P-200820/489
Improper Authentication	07-Aug-20	8.3	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to bypass authentication via a web-administration request that lacks a password parameter. **CVE ID : CVE-2020-15055**	N/A	H-TP--TL-P-200820/490
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Aug-20	2.3	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the same network to conduct persistent XSS attacks by leveraging administrative privileges to set a crafted server name. **CVE ID : CVE-2020-15056**	N/A	H-TP--TL-P-200820/491
Improper Input Validation	07-Aug-20	6.1	TP-Link USB Network Server TL-PS310U devices before 2.079.000.t0210 allow an attacker on the	N/A	H-TP--TL-P-200820/492

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			same network to denial-of-service the device via long input values. **CVE ID : CVE-2020-15057**		
Yokogawa					
centum_cs_3000					
Improper Authenticati on	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**	N/A	H-YOK-CENT-200820/493
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors.	N/A	H-YOK-CENT-200820/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5609		
centum_vp					
Improper Authenticati on	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**	N/A	H-YOK-CENT-200820/495
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **CVE ID : CVE-2020-5609**	N/A	H-YOK-CENT-200820/496
b\/m9000cs					
Improper Authenticati	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM	N/A	H-YOK-B\/M-200820/497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **CVE ID : CVE-2020-5609**	N/A	H-YOK-B\/M-200820/498
b\/m9000vp					
Improper Authenticati on	05-Aug-20	7.5	CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS	N/A	H-YOK-B\/M-200820/499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to bypass authentication and send altered communication packets via unspecified vectors. **CVE ID : CVE-2020-5608**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-Aug-20	7.5	Directory traversal vulnerability in CAMS for HIS CENTUM CS 3000 (includes CENTUM CS 3000 Small) R3.08.10 to R3.09.50, CENTUM VP (includes CENTUM VP Small, Basic) R4.01.00 to R6.07.00, B/M9000CS R5.04.01 to R5.05.01, and B/M9000 VP R6.01.01 to R8.03.01 allows a remote unauthenticated attacker to create or overwrite arbitrary files and run arbitrary commands via unspecified vectors. **CVE ID : CVE-2020-5609**	N/A	H-YOK-B\/M-200820/500
zyzel					
nas326					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and	N/A	H-ZYZ-NAS3-200820/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**		
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and	N/A	H-ZYZ-NAS3-200820/502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**		
nas520					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**	N/A	H-ZYZ-NAS5-200820/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**	N/A	H-ZYZ-NAS5-200820/504
nas540					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0,	N/A	H-ZYZ-NAS5-200820/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**		
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and	N/A	H-ZYZ-NAS5-200820/506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**		
nas542					
Improper Privilege Management	06-Aug-20	9	A backdoor in certain Zyxel products allows remote TELNET access via a CGI script. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and	N/A	H-ZYZ-NAS5-200820/507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13364**		
Improper Privilege Management	06-Aug-20	9	Certain Zyxel products have a locally accessible binary that allows a non-root user to generate a password for an undocumented user account that can be used for a TELNET session as root. This affects NAS520 V5.21(AASZ.4)C0, V5.21(AASZ.0)C0, V5.11(AASZ.3)C0, and V5.11(AASZ.0)C0; NAS542 V5.11(ABAG.0)C0, V5.20(ABAG.1)C0, and V5.21(ABAG.3)C0; NSA325 v2_V4.81(AALS.0)C0 and V4.81(AAAJ.1)C0; NSA310 4.22(AFK.0)C0 and 4.22(AFK.1)C0; NAS326 V5.21(AAZF.8)C0, V5.11(AAZF.4)C0, V5.11(AAZF.2)C0, and V5.11(AAZF.3)C0; NSA310S V4.75(AALH.2)C0; NSA320S V4.75(AANV.2)C0 and V4.75(AANV.1)C0; NSA221 V4.41(AFM.1)C0; and NAS540 V5.21(AATB.5)C0 and V5.21(AATB.3)C0. **CVE ID : CVE-2020-13365**	N/A	H-ZYZ-NAS5-200820/508