Vulnerability Summary for the Week of July 12, 2021

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by Ug-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of Ug-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
echobh -- sharecare	Echo ShareCare 8.15.5 is susceptible to SQL injection vulnerabilities when processing remote input from both authenticated and unauthenticated users, leading to the ability to bypass authentication, exfiltrate Structured Query Language (SQL) records, and manipulate data.	2021-07-13	7.5	CVE-2021-33578 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. It does not perform authentication or authorization checks when accessing a subset of sensitive resources, leading to the ability for unauthenticated users to access pages that are vulnerable to attacks such as SQL injection.	2021-07-13	7.5	CVE-2021-36124 MISC
espruino -- espruino	Buffer overflow vulnerability in function jsvGetStringChars in Espruino before RELEASE_2V09, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22884 MISC
fortinet -- forticlient	An improper symlink following in FortiClient for Mac 6.4.3 and below may allow an non-privileged user to execute arbitrary privileged shell commands during installation phase.	2021-07-12	7.2	CVE-2021-26089 CONFIRM
fortinet -- fortimail	A missing cryptographic step in the implementation of the hash digest algorithm in FortiMail 6.4.0 through 6.4.4, and 6.2.0 through 6.2.7 may allow	2021-07-09	7.5	CVE-2021-24020

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	an unauthenticated attacker to tamper with signed URLs by appending further data which allows bypass of signature verification.			CONFIRM
fortinet -- fortimail	Multiple improper neutralization of special elements of SQL commands vulnerabilities in FortiMail before 6.4.4 may allow a non-authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	7.5	CVE-2021-24007 CONFIRM
golang -- go	golang/go in 1.0.2 fixes all.bash on shared machines. dotest() in src/pkg/debug/gosym/pclntab_test.go creates a temporary file with predicable name and executes it as shell script.	2021-07-09	7.5	CVE-2012-2666 MISC MISC MISC MISC
google -- android	In phNciNfc_RecvMfResp of phNxpExtns_MifareStd.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to	2021-07-14	7.8	CVE-2021-0596 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	remote information disclosure over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181346550			
google -- android	In setNiNotification of GpsNetInitiatedHandler.java, there is a possible permissions bypass due to an empty mutable PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-8.1 Android-9Android ID: A-154319182	2021-07-14	7.2	CVE-2020-0417 MISC
google -- android	In flv extractor, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for	2021-07-14	7.2	CVE-2021-0577 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187161771			
google -- android	In Factory::CreateStrictFunctionMap of factory.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-167389063	2021-07-14	10	CVE-2021-0515 MISC
google -- android	In beginWrite and beginRead of MessageQueueBase.h, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-184963385	2021-07-14	7.2	CVE-2021-0585 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In onCreate of ConfirmConnectActivity, there is a possible remote bypass of user consent due to improper input validation. This could lead to remote (proximal, NFC) escalation of privilege allowing an attacker to deceive a user into allowing a Bluetooth connection with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-176445224	2021-07-14	7.9	CVE-2021-0594 MISC
google -- android	In StreamOut::prepareForWriting of StreamOut.cpp, there is a possible out of bounds write due to a use after 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-8.1 Android-9 Android-10 Android-11Android ID: A-185259758	2021-07-14	7.2	CVE-2021-0587 MISC
google -- android	In BTM_TryAllocateSCN of btm_scn.cc, there is a possible out of bounds write	2021-07-14	7.2	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	due to an incorrect bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-180939982			0589 MISC
google -- android	In various functions in WideVine, there are possible out of bounds writes due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-188061006	2021-07-14	9.3	CVE-2021-0592 MISC
google -- android	In several functions of the V8 library, there is a possible use after free due to a race condition. This could lead to remote code execution in an unprivileged process with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions:	2021-07-14	9.3	CVE-2021-0514 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Android-10 Android-9 Android-11 Android-8.1Android ID: A-162604069			
google -- android	In onCreateOptionsMenu of WifiNetworkDetailsFragment.java, there is a possible way for guest users to view and modify Wi-Fi settings for all configured APs due to a permissions bypass. 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-11Android ID: A-177573895	2021-07-14	7.2	CVE-2021-0602 MISC
halo -- halo	Remote Code Executon vulnerability in Halo 0.4.3 via the remoteAddr and themeName parameters.	2021-07-12	7.5	CVE-2020-18980 MISC
jsish -- jsish	Integer overflow vulnerability in function Jsi_ObjSetLength in jsish before 3.0.6,	2021-07-13	7.5	CVE-2020-22875

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows remote attackers to execute arbitrary code.			MISC MISC
jsish -- jsish	Integer overflow vulnerability in function Jsi_ObjArraySizer in jsish before 3.0.8, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22874 MISC MISC
jsish -- jsish	Buffer overflow vulnerability in function NumberToPrecisionCmd in jsish before 3.0.7, allows remote attackers to execute arbitrary code.	2021-07-13	7.5	CVE-2020-22873 MISC
kaseya -- vsa	Kaseya VSA before 9.5.5 allows remote code execution.	2021-07-09	7.5	CVE-2021-30118 MISC
kramerav -- viaware	KramerAV VIAWare, all tested versions, allow privilege escalation through misconfiguration of sudo. Sudoers permits running of multiple dangerous	2021-07-12	7.5	CVE-2021-35064 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	commands, including unzip, systemctl and dpkg.			
linux -- linux_kernel	An out-of-bounds memory write flaw was found in the Linux kernel's joystick devices subsystem in versions before 5.9-rc1, in the way the user calls ioctl JSIOCSBTNMAP. This flaw allows a local user to crash the system or possibly escalate their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	2021-07-09	7.2	CVE-2021-3612 MISC MISC
linuxptp_project -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. A missing length check when forwarding a PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before	2021-07-09	8	CVE-2021-3570 MISC DEBIAN FEDORA FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1.			
metinfo -- metinfo	SQL Injection vulnerability in Metinfo 7.0.0beta in index.php.	2021-07-12	7.5	CVE-2020-21132 MISC MISC
metinfo -- metinfo	SQL Injection vulnerability in Metinfo 7.0.0 beta in member/getpassword.php?lang=cn&a=dovalid.	2021-07-12	7.5	CVE-2020-21133 MISC MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31196, CVE-2021-34473.	2021-07-14	7.5	CVE-2021-31206 MISC
microsoft -- windows_10	Windows Kernel Elevation of Privilege Vulnerability This CVE ID is unique	2021-07-14	7.2	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	from CVE-2021-31979, CVE-2021-34514.			33771 MISC
microsoft -- windows_10	Windows Security Account Manager Remote Protocol Security Feature Bypass Vulnerability	2021-07-14	7.5	CVE-2021-33757 MISC
microsoft -- windows_10	Windows Secure Kernel Mode Security Feature Bypass Vulnerability	2021-07-14	7.2	CVE-2021-33744 MISC
microsoft -- windows_10	Windows Kernel Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33771, CVE-2021-34514.	2021-07-14	7.2	CVE-2021-31979 MISC
microsoft -- windows_10	Windows Media Remote Code Execution Vulnerability	2021-07-14	9.3	CVE-2021-33740 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. Nextcloud Server supports application specific tokens for authentication purposes. These tokens are supposed to be granted to a specific applications (e.g. DAV sync clients), and can also be configured by the user to not have any filesystem access. Due to a lacking permission check, the tokens were able to change their own permissions in versions prior to 19.0.13, 20.0.11, and 21.0.3. Thus fileystem limited tokens were able to grant themselves access to the filesystem. The issue is patched in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds aside from upgrading.	2021-07-12	7.5	CVE-2021-32688 MISC CONFIRM MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, webauthn tokens were not deleted after a user has been deleted. If a victim reused an earlier used username, the previous user could gain access to their account.	2021-07-12	7.5	CVE-2021-32726 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.			
ninjateam -- filebird	The Filebird Plugin 4.7.3 introduced a SQL injection vulnerability as it is making SQL queries without escaping user input data from a HTTP post request. This is a major vulnerability as the user input is not escaped and passed directly to the get_col function and it allows SQL injection. The Rest API endpoint which invokes this function also does not have any required permissions/authentication and can be accessed by an anonymous user.	2021-07-12	7.5	CVE-2021-24385 CONFIRM MISC
putil-merge_project -- putil-merge	Prototype pollution vulnerability in 'putil-merge' versions1.0.0 through 3.6.6 allows attacker to cause a denial of service and may lead to remote code execution.	2021-07-14	7.5	CVE-2021-25953 MISC
python -- pillow	Pillow through 8.2.0 and PIL (aka Python Imaging Library) through 1.1.7 allow an	2021-07-13	7.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to pass controlled parameters directly into a convert function to trigger a buffer overflow in Convert.c.			34552 MISC MISC
qualcomm -- apq8009w_firmware	Buffer overflow in modem due to improper array index check before copying into it in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearables	2021-07-13	10	CVE-2020-11307 CONFIRM
qualcomm -- apq8017_firmware	Improper length check of public exponent in RSA import key function could cause memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1890 CONFIRM
qualcomm -- apq8017_firmware	Incorrect handling of pointers in trusted application key import mechanism could cause memory corruption in Snapdragon	2021-07-13	7.2	CVE-2021-1886

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables			CONFIRM
qualcomm -- apq8017_firmware	Possible buffer overflow due to lack of length check in Trusted Application in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1889 CONFIRM
qualcomm -- apq8017_firmware	Memory corruption in key parsing and import function due to double freeing the same heap allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1888 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- aqt1000_firmware	Possible buffer overflow due to improper validation of buffer length while processing fast boot commands in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-07-13	7.2	CVE-2021-1931 CONFIRM
qualcomm -- aqt1000_firmware	Use after free can occur due to improper handling of response from firmware in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	7.2	CVE-2021-1940 CONFIRM
qualcomm -- aqt1000_firmware	Possible buffer overflow due to lack of parameter length check during MBSSID scan IE parse in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	10	CVE-2021-1965 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- netweaver_as_abap	A function module of SAP NetWeaver AS ABAP (Reconciliation Framework), versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 75A, 75B, 75B, 75C, 75D, 75E, 75F, allows a high privileged attacker to inject code that can be executed by the application. An attacker could thereby delete some critical information and could make the SAP system completely unavailable.	2021-07-14	7.5	CVE-2021-33678 MISC MISC
solarwinds -- dameware_mini_remote_control	In SolarWinds DameWare Mini Remote Control Server 12.0.1.200, insecure file permissions allow file deletion as SYSTEM.	2021-07-13	9.4	CVE-2021-31217 MISC MISC
totaljs -- total.js	The package total.js before 3.4.9 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.	2021-07-12	7.5	CVE-2021-23389 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
totaljs -- total4	The package total4 before 0.0.43 are vulnerable to Arbitrary Code Execution via the U.set() and U.get() functions.	2021-07-12	7.5	CVE-2021-23390 MISC MISC MISC
wms_project -- wms	SQL Injection in WMS v1.0 allows remote attackers to execute arbitrary code via the "username" parameter in the component "chkuser.php".	2021-07-12	7.5	CVE-2020-18544 MISC
wpdevart -- poll\,_survey\,_questionnaire_and_voting_system	The Poll, Survey, Questionnaire and Voting system WordPress plugin before 1.5.3 did not sanitise, escape or validate the date_answers[] POST parameter before using it in a SQL statement when sending a Poll result, allowing unauthenticated users to perform SQL Injection attacks	2021-07-12	7.5	CVE-2021-24442 CONFIRM MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apache -- ant	When reading a specially crafted TAR archive an Apache Ant build can be made to allocate large amounts of memory that finally leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	2021-07-14	4.3	CVE-2021-36373 MISC MISC MLIST MLIST MLIST
apache -- ant	When reading a specially crafted ZIP archive, or a derived formats, an Apache Ant build can be made to allocate large amounts of memory that leads to an out of memory error, even for small inputs. This can be used to disrupt builds using Apache Ant. Commonly used derived formats from ZIP archives are for instance JAR files and many office files. Apache Ant prior to 1.9.16 and 1.10.11 were affected.	2021-07-14	4.3	CVE-2021-36374 MISC MISC MLIST MLIST MLIST
apache -- tomcat	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when	2021-07-12	5	CVE-2021-33037 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	used with a reverse proxy. Specifically: - Tomcat incorrectly ignored the transfer encoding header if the client declared it would only accept an HTTP/1.0 response; - Tomcat honoured the identify encoding; and - Tomcat did not ensure that, if present, the chunked encoding was the final encoding.			
apache -- tomcat	A vulnerability in Apache Tomcat allows an attacker to remotely trigger a denial of service. An error introduced as part of a change to improve error handling during non-blocking I/O meant that the error flag associated with the Request object was not reset between requests. This meant that once a non-blocking I/O error occurred, all future requests handled by that request object would fail. Users were able to trigger non-blocking I/O errors, e.g. by dropping a connection, thereby creating the possibility of triggering a DoS. Applications that do not use non-blocking I/O are not exposed to this vulnerability. This issue affects Apache Tomcat 10.0.3 to 10.0.4; 9.0.44; 8.5.64.	2021-07-12	5	CVE-2021-30639 MISC MLIST MLIST
artifex -- mujs	Buffer overflow vulnerability in function jsG_markobject in jsgc.c in mujs before 1.0.8, allows remote attackers to cause a denial of service.	2021-07-13	5	CVE-2020-22886 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
artifex -- mujs	Buffer overflow vulnerability in mujs before 1.0.8 due to recursion in the GC scanning phase, allows remote attackers to cause a denial of service.	2021-07-13	5	CVE-2020-22885 MISC
autodesk -- design_review	A maliciously crafted PDF, PICT or TIFF file can be used to write beyond the allocated buffer while parsing PDF, PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27036 MISC
autodesk -- design_review	A maliciously crafted TIFF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read and write beyond allocated boundaries when parsing the TIFF file. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27039 MISC
autodesk -- design_review	A Type Confusion vulnerability in Autodesk 2018, 2017, 2013, 2012, 2011 can occur when processing a maliciously crafted PDF file. An attacker can leverage this to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27038 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- design_review	A maliciously crafted PNG, PDF or DWF file in Autodesk 2018, 2017, 2013, 2012, 2011 can be used to attempt to free an object that has already been freed while parsing them. This vulnerability can be exploited by remote attackers to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27037 MISC
autodesk -- design_review	A heap-based buffer overflow could occur while parsing PICT or TIFF files in Autodesk 2018, 2017, 2013, 2012, 2011. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27034 MISC
autodesk -- design_review	A maliciously crafted TIFF, PDF, PICT or DWF files in Autodesk 2018, 2017, 2013, 2012, 2011 can be forced to read beyond allocated boundaries when parsing the TIFF, PDF, PICT or DWF files. This vulnerability can be exploited to execute arbitrary code.	2021-07-09	6.8	CVE-2021-27035 MISC
axiosys -- bento4	A buffer overflow vulnerability in Ap4ElstAtom.cpp of Bento 1.5.1-628 leads to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19719 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a direct copy to NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19722 MISC
axiosys -- bento4	An unhandled memory allocation failure in Core/AP4IkmsAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19720 MISC
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap4Atom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19718 MISC
axiosys -- bento4	An unhandled memory allocation failure in Core/Ap48bdlAtom.cpp of Bento 1.5.1-628 causes a NULL pointer dereference, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19717 MISC
axiosys -- bento4	A heap buffer overflow vulnerability in Ap4TrunAtom.cpp of Bento 1.5.1-628 may lead to an	2021-07-13	4.3	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	out-of-bounds write while running mp42aac, leading to system crashes and a denial of service (DOS).			19721 MISC
baidu -- umeditor	Cross Site Scripting (XSS) vulnerability in umeditor v1.2.3 via /public/common/umeditor/php/getcontent.php.	2021-07-14	4.3	CVE-2020-18145 MISC
bookingcore -- booking_core	The “Subscribe” feature in Ultimate Booking System Booking Core 1.7.0 is vulnerable to CSV formula injection. The input containing the excel formula is not being sanitized by the application. As a result when admin in backend download and open the csv, content of the cells are executed.	2021-07-14	6.8	CVE-2020-25445 MISC
bookingcore -- booking_core	Cross Site Request Forgery (CSRF) vulnerability in Booking Core - Ultimate Booking System Booking Core 1.7.0 . The CSRF token is not being validated when the request is sent as a GET method. This results in an unauthorized change in the user's email ID, which can later be used to reset the password. The new password will be sent to a modified email ID.	2021-07-14	4.3	CVE-2020-27379 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
brave -- brave	In Brave Desktop between versions 1.17 and 1.26.60, when adblocking is enabled and a proxy browser extension is installed, the CNAME adblocking feature issues DNS requests that used the system DNS settings instead of the extension's proxy settings, resulting in possible information disclosure.	2021-07-12	4.3	CVE-2021-22916 MISC
brave -- browser	Brave Browser Desktop between versions 1.17 and 1.20 is vulnerable to information disclosure by way of DNS requests in Tor windows not flowing through Tor if adblocking was enabled.	2021-07-12	4.3	CVE-2021-22917 MISC
codeblab -- glass	The Glass WordPress plugin through 1.3.2 does not sanitise or escape its "Glass Pages" setting before outputting in a page, leading to a Stored Cross-Site Scripting issue. Furthermore, the plugin did not have CSRF check in place when saving its settings, allowing the issue to be exploited via a CSRF attack.	2021-07-12	4.3	CVE-2021-24434 CONFIRM
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	2021-07-12	4.6	CVE-2021-21590 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 do not exit on failed Initialization. A local authenticated Service user could potentially exploit this vulnerability to escalate privileges.	2021-07-12	4.6	CVE-2021-21589 MISC
dell -- emc_unity_operating_environment	Dell EMC Unity, Unity XT, and UnityVSA versions prior to 5.1.0.0.5.394 contain a plain-text password storage vulnerability. A local malicious user with high privileges may use the exposed password to gain access with the privileges of the compromised user.	2021-07-12	4.6	CVE-2021-21591 MISC
dell -- powerflex_presentation_server	Dell EMC PowerFlex, v3.5.x contain a Cross-Site WebSocket Hijacking Vulnerability in the Presentation Server/WebUI. An unauthenticated attacker could potentially exploit this vulnerability by tricking the user into performing unwanted actions on the Presentation Server and perform which may lead to configuration changes.	2021-07-12	4.3	CVE-2021-21588 MISC
delta_project -- delta	dandavison delta before 0.8.3 on Windows resolves an executable's pathname as a relative path from the current directory.	2021-07-13	4.4	CVE-2021-36376 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
devolutions -- devolutions_server	Devolutions Server before 2021.1.18, and LTS before 2020.3.20, allows attackers to intercept private keys via a man-in-the-middle attack against the connections/partial endpoint (which accepts cleartext).	2021-07-12	4.3	CVE-2021-36382 MISC
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The TextReader feature in General/TextReader/TextReader.cfm is susceptible to a local file inclusion vulnerability when processing remote input in the textFile parameter from an authenticated user, leading to the ability to read arbitrary files on the server filesystems as well any files accessible via Universal Naming Convention (UNC) paths.	2021-07-13	4	CVE-2021-36123 MISC
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The UnzipFile feature in Access/EligFeedParse_Sup/UnzipFile_Upd.cfm is susceptible to a command argument injection vulnerability when processing remote input in the	2021-07-13	6.5	CVE-2021-36122 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	zippass parameter from an authenticated user, leading to the ability to inject arbitrary arguments to 7z.exe.			
echobh -- sharecare	An issue was discovered in Echo ShareCare 8.15.5. The file-upload feature in Access/DownloadFeed_Mnt/FileUpload_Upd.cfm is susceptible to an unrestricted upload vulnerability via the name1 parameter, when processing remote input from an authenticated user, leading to the ability for arbitrary files to be written to arbitrary filesystem locations via ../ Directory Traversal on the Z: drive (a hard-coded drive letter where ShareCare application files reside) and remote code execution as the ShareCare service user (NT AUTHORITY\SYSTEM).	2021-07-13	6.5	CVE-2021-36121 MISC
edgexfoundry -- edgex_foundry	EdgeX Foundry is an open source project for building a common open framework for internet-of-things edge computing. A vulnerability exists in the Edinburgh, Fuji, Geneva, and Hanoi versions of the software. When the EdgeX API gateway is configured for OAuth2 authentication and a proxy user is created, the client_id and client_secret required to obtain an OAuth2 authentication token are set to the username of the proxy user. A remote network attacker can then perform a dictionary-based password attack on the OAuth2 token	2021-07-09	5.8	CVE-2021-32753 MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	endpoint of the API gateway to obtain an OAuth2 authentication token and use that token to make authenticated calls to EdgeX microservices from an untrusted network. OAuth2 is the default authentication method in EdgeX Edinburgh release. The default authentication method was changed to JWT in Fuji and later releases. Users should upgrade to the EdgeX Ireland release to obtain the fix. The OAuth2 authentication method is disabled in Ireland release. If unable to upgrade and OAuth2 authentication is required, users should create OAuth2 users directly using the Kong admin API and forgo the use of the `security-proxy-setup` tool to create OAuth2 users.			
edifecs -- transaction_management	In Edifecs Transaction Management through 2021-07-12, an unauthenticated user can inject arbitrary text into a user's browser via logon.jsp?logon_error= on the login screen of the Web application.	2021-07-12	5	CVE-2021-36381 MISC MISC
element-it -- http_commander	A Directory Traversal vulnerability in the Unzip feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to write files to arbitrary directories via relative paths in ZIP archives.	2021-07-14	4	CVE-2021-33211 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
element-it -- http_commander	An SSRF vulnerability in the "Upload from URL" feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to retrieve HTTP and FTP files from the internal server network by inserting an internal address.	2021-07-14	4	CVE-2021-33213 MISC MISC
esri -- arcgis_server	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	2021-07-10	4.3	CVE-2021-29107 CONFIRM
esri -- arcgis_server	A reflected Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user’s browser.	2021-07-10	4.3	CVE-2021-29106 CONFIRM
esri -- arcgis_server	A Server-Side Request Forgery (SSRF) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote, unauthenticated attacker to forge GET requests to arbitrary URLs from the system, potentially leading to network enumeration or facilitating other attacks.	2021-07-11	6.4	CVE-2021-29102 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
esri -- arcgis_server	A stored Cross Site Scripting (XXS) vulnerability in ArcGIS Server Manager version 10.8.1 and below may allow a remote unauthenticated attacker to pass and store malicious strings in the ArcGIS Server Manager application.	2021-07-11	4.3	CVE-2021-29104 CONFIRM
esri -- arcgis_server	A reflected Cross Site Scripting (XXS) vulnerability in ArcGIS Server version 10.8.1 and below may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the user's browser.	2021-07-11	4.3	CVE-2021-29103 CONFIRM
eventespresso -- event_espresso	A cross-site scripting (XSS) vulnerability in wp-content/plugins/event-espresso-core-reg/admin_pages/messages/templates/ee_msg_admin_overview.template.php in the Event Espresso Core plugin before 4.10.7.p for WordPress allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2021-07-13	4.3	CVE-2020-26153 MISC MISC
exiv2 -- exiv2	A buffer overflow vulnerability in the Databuf function in types.cpp of Exiv2 v0.27.1 leads to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19716 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
exiv2 -- exiv2	An integer overflow vulnerability in the getUShort function of Exiv2 0.27.1 results in segmentation faults within the application, leading to a denial of service (DOS).	2021-07-13	4.3	CVE-2020-19715 MISC
fetchdesigns -- sign-up_sheets	The Sign-up Sheets WordPress plugin before 1.0.14 does not not sanitise or validate the Sheet title when generating the CSV to export, which could lead to a CSV injection issue	2021-07-12	6	CVE-2021-24441 CONFIRM
fortinet -- fortiap	An improper neutralization of special elements used in an OS Command vulnerability in FortiAP's console 6.4.1 through 6.4.5 and 6.2.4 through 6.2.5 may allow an authenticated attacker to execute unauthorized commands by running the kdbg CLI command with specifically crafted arguments.	2021-07-09	4.6	CVE-2021-26106 CONFIRM
fortinet -- fortimail	A missing release of memory after its effective lifetime vulnerability in the Webmail of FortiMail 6.4.0 through 6.4.4 and 6.2.0 through 6.2.6 may allow an unauthenticated remote attacker to exhaust available memory via specifically crafted login requests.	2021-07-12	5	CVE-2021-26090 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortimail	An improper neutralization of special elements used in an OS Command vulnerability in the administrative interface of FortiMail before 6.4.4 may allow an authenticated attacker to execute unauthorized commands via specifically crafted HTTP requests.	2021-07-12	6.5	CVE-2021-24015 CONFIRM
fortinet -- fortimail	A missing cryptographic step in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an unauthenticated attacker who intercepts the encrypted messages to manipulate them in such a way that makes the tampering and the recovery of the plaintexts possible.	2021-07-09	5	CVE-2021-26100 CONFIRM
fortinet -- fortimail	Multiple Path traversal vulnerabilities in the Webmail of FortiMail before 6.4.4 may allow a regular user to obtain unauthorized access to files and data via specifically crafted web requests.	2021-07-12	4	CVE-2021-24013 CONFIRM
fortinet -- fortimail	Missing cryptographic steps in the Identity-Based Encryption service of FortiMail before 7.0.0 may allow an attacker who comes in possession of the encrypted master keys to compromise their confidentiality by observing a few invariant properties of the ciphertext.	2021-07-12	4	CVE-2021-26099 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
fortinet -- fortimail	Multiple instances of incorrect calculation of buffer size in the Webmail and Administrative interface of FortiMail before 6.4.5 may allow an authenticated attacker with regular webmail access to trigger a buffer overflow and to possibly execute unauthorized code or commands via specifically crafted HTTP requests.	2021-07-09	6.5	CVE-2021-22129 CONFIRM
fortinet -- fortisandbox	A concurrent execution using shared resource with improper synchronization ('race condition') in the command shell of FortiSandbox before 3.2.2 may allow an authenticated attacker to bring the system into an unresponsive state via specifically orchestrated sequences of commands.	2021-07-09	6.3	CVE-2020-29014 CONFIRM
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 produce incorrect PDF document signatures because the certificate name, document owner, and signature author are mishandled.	2021-07-09	4.3	CVE-2021-33795 MISC
foxitsoftware -- foxit_reader	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write via a crafted /Size key in the Trailer dictionary.	2021-07-09	6.8	CVE-2021-33792 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
getambassador -- emissary-ingress	Emissary-Ingress (formerly Ambassador API Gateway) through 1.13.9 allows attackers to bypass client certificate requirements (i.e., mTLS cert_required) on backend upstreams when more than one TLSContext is defined and at least one configuration exists that does not require client certificate authentication. The attacker must send an SNI specifying an unprotected backend and an HTTP Host header specifying a protected backend. (2.x versions are unaffected. 1.x versions are unaffected with certain configuration settings involving prune_unreachable_routes and a wildcard Host resource.)	2021-07-09	4.3	CVE-2021-36371 MISC MISC
google -- android	In handleSendStatusChangeBroadcast of WifiDisplayAdapter.java, there is a possible leak of location-sensitive data due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176541017	2021-07-14	4.9	CVE-2021-0518 MISC
google -- android	In onCreate of DevicePickerFragment.java, there is a possible way to trick the user to select an unwanted bluetooth device due to a tapjacking/overlay attack. This	2021-07-14	6.9	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-182584940			0586 MISC
google -- android	In processInboundMessage of MceStateMachine.java, there is a possible SMS disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9Android ID: A-177238342	2021-07-14	4.9	CVE-2021-0588 MISC
google -- android	In onCreate of PermissionActivity.java, there is a possible permission bypass due to Confusing UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174495520	2021-07-14	4.4	CVE-2021-0441 MISC
google -- android	In onCreate of DeviceAdminAdd.java, there is a possible way to mislead a user to activate a device admin app due to improper input validation. This could	2021-07-14	6.9	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-179042963			0600 MISC
google -- android	In encodeFrames of avc_enc_fuzzer.cpp, there is a possible out of bounds write due to a double free. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-180643802	2021-07-14	4.9	CVE-2021-0601 MISC
google -- android	In onCreate of ContactSelectionActivity.java, there is a possible way to get access to contacts without permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-182809425	2021-07-14	4.4	CVE-2021-0603 MISC
google -- android	In sendNetworkConditionsBroadcast of NetworkMonitor.java, there is a possible way for a	2021-07-14	4.9	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileged app to receive WiFi BSSID and SSID without location permissions due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-175213041			0590 MISC
google -- android	In onPackageAddedInternal of PermissionManagerService.java, there is possible access to external storage due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-171430330	2021-07-14	4.6	CVE-2021-0486 MISC
google -- android	In scheduleTimeoutLocked of NotificationRecord.java, there is a possible disclosure of a sensitive identifier via broadcasted intent due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-175614289	2021-07-14	4.9	CVE-2021-0599 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	In notifyProfileAdded and notifyProfileRemoved of SipService.java, there is a possible way to retrieve SIP account names due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-176496502	2021-07-14	4.9	CVE-2021-0597 MISC
halo -- halo	File Deletion vulnerability in Halo 0.4.3 via delBackup.	2021-07-12	6.4	CVE-2020-19038 MISC
halo -- halo	Incorrect Access Control vulnearbility in Halo 0.4.3, which allows a malicious user to bypass encrption to view encrpted articles via cookies.	2021-07-12	5	CVE-2020-19037 MISC
halo -- halo	Cross Siste Scripting (XSS) vulnerablity in Halo 0.4.3 via the X-forwarded-for Header parameter.	2021-07-12	4.3	CVE-2020-18979 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
halo -- halo	SSRF vulnerability in Halo <=1.3.2 exists in the SMTP configuration, which can detect the server intranet.	2021-07-12	5	CVE-2020-23079 MISC
hms-networks -- ecatcher	In HMS Ewon eCatcher through 6.6.4, weak filesystem permissions could allow malicious users to access files that could lead to sensitive information disclosure, modification of configuration files, or disruption of normal system operation.	2021-07-09	6	CVE-2021-33214 MISC MISC MISC MISC
hmtalk -- daviewindy	DaviewIndy v8.98.7.0 and earlier versions have a Integer overflow vulnerability, triggered when the user opens a malformed format file that is mishandled by DaviewIndy. Attackers could exploit this and arbitrary code execution.	2021-07-12	6.8	CVE-2020-7872 MISC
huawei -- harmonyos	A component of the HarmonyOS 2.0 has a Null Pointer Dereference Vulnerability. Local attackers may exploit this vulnerability to cause system denial of service.	2021-07-14	4.9	CVE-2021-22318 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could allow an authenticated user gain escalated privilesges due to improper application permissions. IBM X-Force ID: 196308.	2021-07-13	6.5	CVE-2021-20423 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could disclose sensitive information to a malicious attacker by accessing data stored in memory. IBM X-Force ID: 196304.	2021-07-13	5	CVE-2021-20422 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 195361.	2021-07-13	4.3	CVE-2021-20369 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 uses weaker than expected cryptographic algorithms that could allow an	2021-07-13	5	CVE-2021-20360

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker to decrypt highly sensitive information. IBM X-Force ID: 195031.			CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. X-Force ID: 196309.	2021-07-13	4	CVE-2021-20424 XF CONFIRM
ibm -- event_streams	IBM Event Streams 10.0, 10.1, 10.2, and 10.3 could allow a user the CA private key to create their own certificates and deploy them in the cluster and gain privileges of another user. IBM X-Force ID: 203450.	2021-07-12	6.5	CVE-2021-29792 CONFIRM XF
ibm -- guardium_data_encryption	IBM Guardium Data Encryption (GDE) 3.0.0.2 could allow a user to bruce force sensitive information due to not properly limiting the number of interactions. IBM X-Force ID: 196216.	2021-07-12	4	CVE-2021-20414 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 200966.	2021-07-09	4.3	CVE-2021-29712 CONFIRM XF
ibm -- infosphere_information_server	IBM InfoSphere Information Server 11.7 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: 201164.	2021-07-09	6.5	CVE-2021-29730 XF CONFIRM
ibm -- mq_appliance	IBM MQ Appliance 9.1 and 9.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 191815.	2021-07-12	6.8	CVE-2020-4938 CONFIRM XF
ibm -- tivoli_netcool\/impact	IBM Tivoli Netcool/Impact 7.1.0.20 and 7.1.0.21 uses an insecure SSH server configuration which enables weaker than expected cryptographic algorithms that	2021-07-12	5	CVE-2021-29794

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 203556.			XF CONFIRM
icinga -- icinga	Icinga Web 2 is an open source monitoring web interface, framework, and command-line interface. A vulnerability in which custom variables are exposed to unauthorized users exists between versions 2.0.0 and 2.8.2. Custom variables are user-defined keys and values on configuration objects in Icinga 2. These are commonly used to reference secrets in other configurations such as check commands to be able to authenticate with a service being checked. Icinga Web 2 displays these custom variables to logged in users with access to said hosts or services. In order to protect the secrets from being visible to anyone, it's possible to setup protection rules and blacklists in a user's role. Protection rules result in `***` being shown instead of the original value, the key will remain. Backlists will hide a custom variable entirely from the user. Besides using the UI, custom variables can also be accessed differently by using an undocumented URL parameter. By adding a parameter to the affected routes, Icinga Web 2 will show these columns additionally in the respective list. This parameter is also respected when	2021-07-12	4	CVE-2021-32747 MISC MISC CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	exporting to JSON or CSV. Protection rules and blacklists however have no effect in this case. Custom variables are shown as-is in the result. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, one may set up a restriction to hide hosts and services with the custom variable in question.			
ipfire -- ipfire	Lightning Wire Labs IPFire 2.21 (x86_64) - Core Update 130 is affected by: Cross Site Scripting (XSS). The impact is: Session Hijacking (local). The component is: Affected at Routing configuration via the "Remark" text box or "remark" parameter. The attack vector is: Attacker need to craft the malicious javascript code.	2021-07-12	4.3	CVE-2020-19204 MISC MISC
jsish -- jsish	Stack overflow vulnerability in function jsi_evalcode_sub in jsish before 3.0.18, allows remote attackers to cause a Denial of Service via a crafted value to the execute parameter.	2021-07-13	5	CVE-2020-22907 MISC
kaseya -- vsa	SQL injection exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30117 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
kaseya -- vsa	Local file inclusion exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30121 MISC
kaseya -- vsa	Kaseya VSA through 9.5.7 allows attackers to bypass the 2FA requirement.	2021-07-09	5	CVE-2021-30120 MISC
kaseya -- vsa	An XML External Entity (XXE) issue exists in Kaseya VSA before 9.5.6.	2021-07-09	6.5	CVE-2021-30201 MISC
linecorp -- line	LINE client for iOS before 10.16.3 allows cross site script with specific header in WebView.	2021-07-13	4.3	CVE-2021-36214 MISC
linuxfoundation -- grpc_swift	Mismanaged state in GRPCWebToHTTP2ServerCodec.swift in gRPC Swift	2021-07-09	5	CVE-2021-36153

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	1.1.0 and 1.1.1 allows remote attackers to deny service by sending malformed requests.			MISC MISC MISC
linuxfoundation -- grpc_swift	LengthPrefixedMessageReader in gRPC Swift 1.1.0 and earlier allocates buffers of arbitrary length, which allows remote attackers to cause uncontrolled resource consumption and deny service.	2021-07-09	5	CVE-2021-36155 MISC MISC MISC
linuxfoundation -- grpc_swift	HTTP2ToRawGRPCServerCodec in gRPC Swift 1.1.1 and earlier allows remote attackers to deny service via the delivery of many small messages within a single HTTP/2 frame, leading to Uncontrolled Recursion and stack consumption.	2021-07-09	5	CVE-2021-36154 MISC MISC MISC
linuxptp_project -- linuxptp	A flaw was found in the ptp4l program of the linuxptp package. When ptp4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and	2021-07-09	5.5	CVE-2021-3571 MISC FEDORA

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1.			FEDORA
metinfo -- metinfo	SQL Injection vulnerability in MetInfo 7.0.0beta via admin/?n=language&c=language_web&a=doAddLanguage.	2021-07-12	6.5	CVE-2020-21131 MISC MISC
microfocus -- netiq_advanced_authentication	Multi-Factor Authentication (MFA) functionality can be bypassed, allowing the use of single factor authentication in NetIQ Advanced Authentication versions prior to 6.3 SP4 Patch 1.	2021-07-12	4	CVE-2021-22515 CONFIRM
microsoft -- bing	Microsoft Bing Search Spoofing Vulnerability	2021-07-14	4.3	CVE-2021-33753 MISC
microsoft -- exchange_server	Microsoft Exchange Information Disclosure Vulnerability	2021-07-14	5	CVE-2021-33766

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
microsoft -- exchange_server	Microsoft Exchange Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31206, CVE-2021-34473.	2021-07-14	6.5	CVE-2021-31196 MISC
microsoft -- exchange_server	Microsoft Exchange Server Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34470, CVE-2021-34523.	2021-07-14	5.2	CVE-2021-33768 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33776, CVE-2021-33777.	2021-07-14	6.8	CVE-2021-33778 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33776, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33775 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33776 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-31947, CVE-2021-33775, CVE-2021-33776, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-33777 MISC
microsoft -- hevc_video_extensions	HEVC Video Extensions Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33775, CVE-2021-33776, CVE-2021-33777, CVE-2021-33778.	2021-07-14	6.8	CVE-2021-31947 MISC
microsoft -- open_enclave_software_development_kit	Open Enclave SDK Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33767 MISC
microsoft -- power_bi_report_server	Power BI Remote Code Execution Vulnerability	2021-07-14	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				31984 MISC
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33773, CVE-2021-34445, CVE-2021-34456.	2021-07-14	4.6	CVE-2021-33761 MISC
microsoft -- windows_10	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33772, CVE-2021-34490.	2021-07-14	5	CVE-2021-31183 MISC
microsoft -- windows_10	Windows Desktop Bridge Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33759 MISC
microsoft -- windows_10	Storage Spaces Controller Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-34460, CVE-2021-34510, CVE-2021-34512, CVE-2021-34513.	2021-07-14	4.6	CVE-2021-33751 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Projected File System Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33743 MISC
microsoft -- windows_10	Windows Event Tracing Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33774 MISC
microsoft -- windows_10	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-33761, CVE-2021-34445, CVE-2021-34456.	2021-07-14	4.6	CVE-2021-33773 MISC
microsoft -- windows_10	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2021-07-14	4.6	CVE-2021-33784 MISC
microsoft -- windows_10	Windows Authenticode Spoofing Vulnerability	2021-07-14	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				33782 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33750, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33752 MISC
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33755.	2021-07-14	4	CVE-2021-33758 MISC
microsoft -- windows_10	Windows TCP/IP Driver Denial of Service Vulnerability This CVE ID is unique from CVE-2021-31183, CVE-2021-34490.	2021-07-14	5	CVE-2021-33772 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33750, CVE-2021-33752.	2021-07-14	6.8	CVE-2021-33756 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Hyper-V Denial of Service Vulnerability This CVE ID is unique from CVE-2021-33758.	2021-07-14	5	CVE-2021-33755 MISC
microsoft -- windows_10	Windows SMB Information Disclosure Vulnerability	2021-07-14	4	CVE-2021-33783 MISC
microsoft -- windows_10	Windows AF_UNIX Socket Provider Denial of Service Vulnerability	2021-07-14	5	CVE-2021-33785 MISC
microsoft -- windows_10	Azure AD Security Feature Bypass Vulnerability	2021-07-14	5.5	CVE-2021-33781 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33750, CVE-2021-33752, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				33749 MISC
microsoft -- windows_10	Windows DNS Snap-in Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33749, CVE-2021-33752, CVE-2021-33756.	2021-07-14	6.8	CVE-2021-33750 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33754, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6.5	CVE-2021-33780 MISC
microsoft -- windows_server_2008	Windows Key Distribution Center Information Disclosure Vulnerability	2021-07-14	4.3	CVE-2021-33764 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33754, CVE-2021-33780, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6.5	CVE-2021-33746 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_server_2008	Windows DNS Server Denial of Service Vulnerability This CVE ID is unique from CVE-2021-34442, CVE-2021-34444, CVE-2021-34499.	2021-07-14	4	CVE-2021-33745 MISC
microsoft -- windows_server_2008	Windows DNS Server Remote Code Execution Vulnerability This CVE ID is unique from CVE-2021-33746, CVE-2021-33780, CVE-2021-34494, CVE-2021-34525.	2021-07-14	6	CVE-2021-33754 MISC
microsoft -- windows_server_2016	Windows ADFS Security Feature Bypass Vulnerability	2021-07-14	5.5	CVE-2021-33779 MISC
mikrotik -- routeros	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference). NOTE: this is different from CVE-2020-20253 and CVE-2020-20254. All four vulnerabilities in the /nova/bin/lcdstat process are discussed in the CVE-2020-20250 github.com/cq674350529 reference.	2021-07-13	4	CVE-2020-20250 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
mikrotik -- routeros	Mikrotik RouterOs before stable version 6.47 suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).	2021-07-13	4	CVE-2020-20252 MISC
mitre -- caldera	A command injection vulnerability in the sandcat plugin of Caldera 2.3.1 and earlier allows authenticated attackers to execute any command or service.	2021-07-12	6.5	CVE-2020-19907 MISC
moddable -- moddable	Issue was discovered in the fxParserTree function in moddable, allows attackers to cause denial of service via a crafted payload. Fixed in commit 723816ab9b52f807180c99fc69c7d08cf6c6bd61.	2021-07-13	5	CVE-2020-22882 MISC
nextcloud -- nextcloud	Nextcloud Android Client is the Android client for Nextcloud. Clients using the Nextcloud end-to-end encryption feature download the public and private key via an API endpoint. In versions prior to 3.16.1, the Nextcloud Android client skipped a step that involved the client checking if a private key belonged to a previously downloaded public certificate. If the Nextcloud instance served a malicious public key, the	2021-07-12	5	CVE-2021-32727 CONFIRM MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data would be encrypted for this key and thus could be accessible to a malicious actor. The vulnerability is patched in version 3.16.1. As a workaround, do not add additional end-to-end encrypted devices to a user account.			
nextcloud -- nextcloud_mail	Nextcloud Mail is a mail app for Nextcloud. In versions prior to 1.9.6, the Nextcloud Mail application does not, by default, render images in emails to not leak the read state. The privacy filter failed to filter images with a `background-image` CSS attribute. Note that the images were still passed through the Nextcloud image proxy, and thus there was no IP leakage. The issue was patched in version 1.9.6 and 1.10.0. No workarounds are known to exist.	2021-07-12	4	CVE-2021-32707 MISC MISC CONFIRM
nextcloud -- nextcloud_server	Nextcloud Text is a collaborative document editing application that uses Markdown. A cross-site scripting vulnerability is present in versions prior to 19.0.13, 20.0.11, and 21.0.3. The Nextcloud Text application shipped with Nextcloud server used a `text/html` Content-Type when serving files to users. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. The issue was fixed in	2021-07-12	4.3	CVE-2021-32733 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, use a browser that has support for Content-Security-Policy.			
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the shareinfo endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32703 CONFIRM MISC MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public DAV endpoint. This may have allowed an attacker to enumerate potentially valid share tokens or credentials. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32705 MISC MISC CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, filenames where not escaped by default in controllers using `DownloadResponse`. When a user-	2021-07-12	6.8	CVE-2021-32679 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	supplied filename was passed unsanitized into a `DownloadResponse`, this could be used to trick users into downloading malicious files with a benign file extension. This would show in UI behaviours where Nextcloud applications would display a benign file extension (e.g. JPEG), but the file will actually be downloaded with an executable file extension. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. Administrators of Nextcloud instances do not have a workaround available, but developers of Nextcloud apps may manually escape the file name before passing it into `DownloadResponse`.			RM MISC MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.0.11, and 21.0.3, ratelimits are not applied to OCS API responses. This affects any OCS API controller (`OCSController`) using the `@BruteForceProtection` annotation. Risk depends on the installed applications on the Nextcloud Server, but could range from bypassing authentication ratelimits or spamming other Nextcloud users. The vulnerability is patched in versions 19.0.13, 20.0.11, and 21.0.3. No workarounds aside from upgrading are known to exist.	2021-07-12	5	CVE-2021-32678 MISC MISC CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, there was a lack of ratelimiting on the public share link mount endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32741 MISC MISC CONFIRM
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, the Nextcloud Text application shipped with Nextcloud Server returned verbatim exception messages to the user. This could result in a full path disclosure on shared files. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. As a workaround, one may disable the Nextcloud Text application in Nextcloud Server app settings.	2021-07-12	5	CVE-2021-32734 CONFIRM MISC MISC
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions prior to 19.0.13, 20.011, and 21.0.3, default share permissions were not being respected for federated reshares of files and folders. The issue was fixed in versions 19.0.13, 20.0.11, and 21.0.3. There are no known workarounds.	2021-07-12	5	CVE-2021-32725 CONFIRM MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- talk	Nextcloud Talk is a fully on-premises audio/video and chat communication service. In versions prior to 11.2.2, if a user was able to reuse an earlier used username, they could get access to any chat message sent to the previous user with this username. The issue was patched in versions 11.2.2 and 11.3.0. As a workaround, don't allow users to choose usernames themselves. This is the default behaviour of Nextcloud, but some user providers may allow doing so.	2021-07-12	4	CVE-2021-32689 MISC MISC MISC CONFIRM MISC
nodejs -- node.js	Node.js before 16.4.1, 14.17.2, 12.22.2 is vulnerable to an out-of-bounds read when uv__idna_toascii() is used to convert strings to ASCII. The pointer p is read and increased without checking whether it is beyond pe, with the latter holding a pointer to the end of the buffer. This can lead to information disclosures or crashes. This function can be triggered via uv_getaddrinfo().	2021-07-12	6.4	CVE-2021-22918 MISC MISC
nodejs -- node.js	Node.js before 16.4.1, 14.17.2, and 12.22.2 is vulnerable to local privilege escalation attacks under certain conditions on Windows platforms. More specifically, improper configuration of permissions in the installation directory allows an attacker to perform two different escalation attacks: PATH and DLL hijacking.	2021-07-12	4.4	CVE-2021-22921 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openvpn -- openvpn	OpenVPN 3 Core Library version 3.6 and 3.6.1 allows a man-in-the-middle attacker to bypass the certificate authentication by issuing an unrelated server certificate using the same hostname found in the verify-x509-name option in a client configuration.	2021-07-12	5.8	CVE-2021-3547 MISC MISC
panasonic -- fpwin_pro	Panasonic FPWIN Pro, all Versions 7.5.1.1 and prior, allows an attacker to craft a project file specifying a URI that causes the XML parser to access the URI and embed the contents, which may allow the attacker to disclose information that is accessible in the context of the user executing software.	2021-07-09	4.3	CVE-2021-32972 MISC
pbootcms -- pbootcms	Incorrect Access Control vulnerability in PbootCMS 2.0.6 via the list parameter in the update function in upgradecontroller.php.	2021-07-09	4	CVE-2020-22535 MISC
pfsense -- pfsense	Netgate pfSense Community Edition 2.4.4 - p2 (arm64) is affected by: Cross Site Scripting (XSS). The impact is: Session Hijacking, Information Leakage (local). The component is: pfSense Dashboard, Work-on-LAN Service configuration. The attack vector is: Inject the	2021-07-12	4.3	CVE-2020-19203 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious JavaScript code in Description text box or parameter.			
plugin-planet -- prismatic	The Prismatic WordPress plugin before 2.8 does not escape the 'tab' GET parameter before outputting it back in an attribute, leading to a reflected Cross-Site Scripting issue which will be executed in the context of a logged in administrator	2021-07-12	4.3	CVE-2021-24409 CONFIRM
pluginus -- wordpress_meta_data_and_taxonomies_filter	Cross-site request forgery (CSRF) vulnerability in WordPress Meta Data Filter & Taxonomies Filter versions prior to v.1.2.8 and versions prior to v.2.2.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-14	6.8	CVE-2021-20781 MISC MISC MISC
putty -- putty	PuTTY through 0.75 proceeds with establishing an SSH session even if it has never sent a substantive authentication response. This makes it easier for an attacker-controlled SSH server to present a later spoofed authentication prompt (that the attacker can use to capture credential data, and use that data for purposes that are undesired by the client user).	2021-07-09	5.8	CVE-2021-36367 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- apq8009_firmware	Denial of service in SAP case due to improper handling of connections when association is rejected in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	5	CVE-2021-1955 CONFIRM
qualcomm -- apq8053_firmware	Possible out of bound read due to lack of length check of FT sub-elements in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	2021-07-13	5	CVE-2021-1970 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer overflow due to lack of length check in BA request in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-07-13	5	CVE-2021-1907 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer over read due to improper validation of IE size while parsing beacon from peer device in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	2021-07-13	5	CVE-2021-1964

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking			CONFIRM
qualcomm -- apq8053_firmware	Possible buffer out of bound read can occur due to improper validation of TBTT count and length while parsing the beacon response in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1943 CONFIRM
qualcomm -- apq8053_firmware	Possible buffer over read due to improper validation of data pointer while parsing FILS indication IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1954 CONFIRM
qualcomm -- apq8053_firmware	Possible out of bound read due to lack of length check of Bandwidth-NSS IE in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1945 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- aqt1000_firmware	Improper handling of received malformed FTMR request frame can lead to reachable assertion while responding with FTM1 frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1953 CONFIRM
qualcomm -- aqt1000_firmware	Possible assertion due to improper verification while creating and deleting the peer in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1938 CONFIRM
qualcomm -- ar7420_firmware	An assertion can be reached in the WLAN subsystem while using the Wi-Fi Fine Timing Measurement protocol in Snapdragon Wired Infrastructure and Networking	2021-07-13	5	CVE-2021-1887 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
quickjs_project -- quickjs	Buffer Overflow vulnerability in quickjs.c in QuickJS, allows remote attackers to cause denial of service. This issue is resolved in the 2020-07-05 release.	2021-07-13	5	CVE-2020-22876 MISC
redhat -- keycloak	A flaw was found in keycloak-model-infinispan in keycloak versions before 14.0.0 where authenticationSessions map in RootAuthenticationSessionEntity grows boundlessly which could lead to a DoS attack.	2021-07-09	5	CVE-2021-3637 MISC
restsharp -- restsharp	RestSharp < 106.11.8-alpha.0.13 uses a regular expression which is vulnerable to Regular Expression Denial of Service (ReDoS) when converting strings into DateTimes. If a server responds with a malicious string, the client using RestSharp will be stuck processing it for an exceedingly long time. Thus the remote server can trigger Denial of Service.	2021-07-12	5	CVE-2021-27293 MISC MISC
retty -- retty	Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 uses a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app.	2021-07-14	5	CVE-2021-20748 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
retty -- retty	Improper authorization in handler for custom URL scheme vulnerability in Retty App for Android versions prior to 4.8.13 and Retty App for iOS versions prior to 4.11.14 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App.	2021-07-14	4.3	CVE-2021-20747 MISC MISC
rockwellautomation -- micrologix_1100_firmware	Rockwell Automation MicroLogix 1100, all versions, allows a remote, unauthenticated attacker sending specially crafted commands to cause the PLC to fault when the controller is switched to RUN mode, which results in a denial-of-service condition. If successfully exploited, this vulnerability will cause the controller to fault whenever the controller is switched to RUN mode.	2021-07-09	5	CVE-2021-33012 MISC
salonbookingsystem -- salon_booking_system	The Salon booking system WordPress plugin before 6.3.1 does not properly sanitise and escape the First Name field when booking an appointment, allowing low privilege users such as subscriber to set JavaScript in them, leading to a Stored Cross-Site Scripting (XSS) vulnerability. The Payload will then be triggered when an admin visits the "Calendar" page and the malicious script is executed in the admin context.	2021-07-12	4.3	CVE-2021-24429 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes out of bounds write and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	2021-07-14	4.3	CVE-2021-33681 MISC MISC
sap -- 3d_visual_enterprise_viewer	SAP 3D Visual Enterprise Viewer, version - 9, allows a user to open manipulated CGM file received from untrusted sources which causes buffer overflow and causes the application to crash and becoming temporarily unavailable until the user restarts the application.	2021-07-14	4.3	CVE-2021-33680 MISC MISC
sap -- businessobjects_web_intelligence	Under certain conditions, SAP Business Objects Web Intelligence (BI Launchpad) versions - 420, 430, allows an attacker to access jsp source code, through SDK calls, of Analytical Reporting bundle, a part of the frontend application, which would otherwise be restricted.	2021-07-14	4	CVE-2021-33667 MISC MISC
sap -- customer_relationship_management	A missing authority check in SAP CRM, versions - 700, 701, 702, 712, 713, 714, could be leveraged by an	2021-07-14	6.5	CVE-2021-33676

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker with high privileges to compromise confidentiality, integrity, or availability of the system.			MISC MISC
sap -- netweaver_abap	SAP NetWeaver ABAP Server and ABAP Platform, versions - 700, 702, 730, 731, 804, 740, 750, 784, expose functions to external which can lead to information disclosure.	2021-07-14	5	CVE-2021-33677 MISC MISC
sap -- netweaver_application_server_java	When user with insufficient privileges tries to access any application in SAP NetWeaver Administrator (Administrator applications), version - 7.50, no security audit log is created. Therefore, security audit log Integrity is impacted.	2021-07-14	4	CVE-2021-33689 MISC MISC
sap -- netweaver_application_server_java	SAP NetWeaver AS for Java (Http Service Monitoring Filter), versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to send multiple HTTP requests with different method types thereby crashing the filter and making the HTTP server unavailable to other legitimate users leading to denial of service vulnerability.	2021-07-14	5	CVE-2021-33670 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
sap -- netweaver_application_server_java	SAP NetWeaver AS JAVA (Enterprise Portal), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50 reveals sensitive information in one of their HTTP requests, an attacker can use this in conjunction with other attacks such as XSS to steal this information.	2021-07-14	4	CVE-2021-33687 MISC MISC
sap -- netweaver_guided_procedures	SAP NetWeaver Guided Procedures (Administration Workset), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. The impact of missing authorization could result to abuse of functionality restricted to a particular user group, and could allow unauthorized users to read, modify or delete restricted data.	2021-07-14	6.5	CVE-2021-33671 MISC MISC
segment -- is-email	A ReDoS (regular expression denial of service) flaw was found in the Segment is-email package before 1.0.1 for Node.js. An attacker that is able to provide crafted input to the isEmail(input) function may cause an application to consume an excessive amount of CPU.	2021-07-14	5	CVE-2021-36716 MISC CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All	2021-07-13	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13404)			34319 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13442)	2021-07-13	6.8	CVE-2021-34331 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage	2021-07-13	6.8	CVE-2021-34330 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	this vulnerability to execute code in the context of the current process. (ZDI-CAN-13430)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13427)	2021-07-13	6.8	CVE-2021-34329 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13199)	2021-07-13	4.3	CVE-2021-34304 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13422)	2021-07-13	6.8	CVE-2021-34326 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13420)	2021-07-13	6.8	CVE-2021-34324 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of	2021-07-13	6.8	CVE-2021-34323 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13419)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The DL180CoolType.dll library in affected applications lacks proper validation of user-supplied data when parsing PDF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13380)	2021-07-13	6.8	CVE-2021-34316 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing ASM files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13423)	2021-07-13	6.8	CVE-2021-34327 CONFIRM CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13343)	2021-07-13	4.3	CVE-2021-34307 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13356)	2021-07-13	6.8	CVE-2021-34315 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing SGI files. This could result	2021-07-13	6.8	CVE-2021-34314 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13355)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13354)	2021-07-13	6.8	CVE-2021-34313 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13353)	2021-07-13	6.8	CVE-2021-34312 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Mono_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13352)	2021-07-13	6.8	CVE-2021-34311 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13192)	2021-07-13	4.3	CVE-2021-34299 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result	2021-07-13	4.3	CVE-2021-34302 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13197)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13198)	2021-07-13	4.3	CVE-2021-34303 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCT files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13403)	2021-07-13	6.8	CVE-2021-34318 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Solid Edge SE2021 (All Versions < SE2021MP5), Teamcenter Visualization (All versions < V13.2). The plmxmlAdapterSE70.dll library in affected applications lacks proper validation of user-supplied data when parsing PAR files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13424)	2021-07-13	6.8	CVE-2021-34328 CONFIRM CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing PCX files. This could result in an out of bounds write past the fixed-length heap-based buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13402)	2021-07-13	6.8	CVE-2021-34317 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied	2021-07-13	6.8	CVE-2021-34291

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12956)			CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13057)	2021-07-13	6.8	CVE-2021-34296 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-12959)	2021-07-13	6.8	CVE-2021-34292 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The VisDraw.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13414)	2021-07-13	4.3	CVE-2021-34321 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13406)	2021-07-13	4.3	CVE-2021-34320 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Jt981.dll library in affected applications lacks proper validation of user-supplied data when parsing JT files. This could result in an out of	2021-07-13	4.3	CVE-2021-34325 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13421)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in an infinite loop condition that leads to denial of service condition. An attacker could leverage this vulnerability to consume excessive resources. (CNVD-C-2021-79300)	2021-07-13	4.3	CVE-2021-34332 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. A malformed input file could result in double free of an allocated buffer that leads to a crash. An attacker could leverage this vulnerability to cause denial of service condition. (CNVD-C-2021-79295)	2021-07-13	4.3	CVE-2021-34333 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13351)	2021-07-13	6.8	CVE-2021-34310 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13344)	2021-07-13	4.3	CVE-2021-34308 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The JPEG2K_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing J2K files. This could result	2021-07-13	4.3	CVE-2021-34322 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-13416)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13350)	2021-07-13	6.8	CVE-2021-34309 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13024)	2021-07-13	6.8	CVE-2021-34295 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13342)	2021-07-13	6.8	CVE-2021-34306 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13340)	2021-07-13	6.8	CVE-2021-34305 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds write past the end of an allocated structure.	2021-07-13	6.8	CVE-2021-34293 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13020)			
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13196)	2021-07-13	6.8	CVE-2021-34301 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Tiff_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing TIFF files. This could result in an out of bounds write past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13194)	2021-07-13	6.8	CVE-2021-34300 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data prior to performing further free operations on an object when parsing BMP files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13060)	2021-07-13	6.8	CVE-2021-34298 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The Gif_loader.dll library in affected applications lacks proper validation of user-supplied data when parsing GIF files. This could result in an out of bounds read past the end of an allocated buffer. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13023	2021-07-13	6.8	CVE-2021-34294 CONFIRM
siemens -- jt2go	A vulnerability has been identified in JT2Go (All versions < V13.2), Teamcenter Visualization (All versions < V13.2). The BMP_Loader.dll library in affected applications lacks proper validation of user-supplied data when parsing BMP files. This could result in an out of bounds write past the end of an allocated	2021-07-13	6.8	CVE-2021-34297 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	structure. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13059)			
sonicwall -- switch	Multiple Out-of-Bound read vulnerability in SonicWall Switch when handling LLDP Protocol allows an attacker to cause a system instability or potentially read sensitive information from the memory locations.	2021-07-09	6.8	CVE-2021-20024 CONFIRM
stormshield -- endpoint_security	Stormshield Endpoint Security Evolution 2.0.0 through 2.0.2 does not accomplish the intended defense against local administrators who can replace the Visual C++ runtime DLLs (in %WINDIR%\system32) with malicious ones.	2021-07-13	4.6	CVE-2021-35957 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows deleting some resources not currently in use by any security policy by leveraging access to a computer having the administration console installed.	2021-07-13	4.3	CVE-2021-31225 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
tipsandtricks-hq -- software_license_manager	Cross-site request forgery (CSRF) vulnerability in Software License Manager versions prior to 4.4.6 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-07-14	6.8	CVE-2021-20782 MISC MISC MISC
vmware -- cloud_foundation	SFCB (Small Footprint CIM Broker) as used in ESXi has an authentication bypass vulnerability. A malicious actor with network access to port 5989 on ESXi may exploit this issue to bypass SFCB authentication by sending a specially crafted request.	2021-07-13	6.8	CVE-2021-21994 MISC
vmware -- cloud_foundation	OpenSLP as used in ESXi has a denial-of-service vulnerability due a heap out-of-bounds read issue. A malicious actor with network access to port 427 on ESXi may be able to trigger a heap out-of-bounds read in OpenSLP service resulting in a denial-of-service condition.	2021-07-13	5	CVE-2021-21995 MISC
vmware -- thinapp	VMware Thinapp version 5.x prior to 5.2.10 contain a DLL hijacking vulnerability due to insecure loading of DLLs. A malicious actor with non-administrative privileges may exploit this vulnerability to elevate	2021-07-13	6.9	CVE-2021-22000 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	privileges to administrator level on the Windows operating system having VMware ThinApp installed on it.			FULLDISC
voidtools -- everything	HTTP header injection vulnerability in Everything all versions except the Lite version may allow a remote attacker to inject an arbitrary script or alter the website that uses the product via unspecified vectors.	2021-07-14	5.8	CVE-2021-20784 MISC MISC MISC
wayang-cms_project -- wayang-cms	A SQL injection vulnerability in wy_controlls/wy_side_visitor.php of Wayang-CMS v1.0 allows attackers to obtain sensitive database information.	2021-07-14	5	CVE-2020-29147 MISC
wayang-cms_project -- wayang-cms	A cross site scripting (XSS) vulnerability in index.php of Wayang-CMS v1.0 allows attackers to execute arbitrary web scripts or HTML via a constructed payload created by adding the X-Forwarded-For field to the header.	2021-07-14	4.3	CVE-2020-29146 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
wire -- wire	Wire is a collaboration platform. wire-ios-transport handles authentication of requests, network failures, and retries for the iOS implementation of Wire. In the 3.82 version of the iOS application, a new web socket implementation was introduced for users running iOS 13 or higher. This new websocket implementation is not configured to enforce certificate pinning when available. Certificate pinning for the new websocket is enforced in version 3.84 or above.	2021-07-13	4	CVE-2021-32755 CONFIRM
xen-orchestra -- xo-server	Xen Orchestra (with xo-web through 5.80.0 and xo-server through 5.84.0) mishandles authorization, as demonstrated by modified WebSocket resourceSet.getAll data is which the attacker changes the permission field from none to admin. The attacker gains access to data sets such as VMs, Backups, Audit, Users, and Groups.	2021-07-12	4	CVE-2021-36383 MISC
xml\ -- \	It was discovered that the XML::Atom Perl module before version 0.39 did not disable external entities when parsing XML from potentially untrusted sources. This may allow attackers to gain read access to otherwise protected resources, depending on how the library is used.	2021-07-09	5	CVE-2012-1102 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
xmlsoft -- libxml2	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.	2021-07-09	4	CVE-2021-3541 MISC
yop-poll -- yop_poll	In the YOP Poll WordPress plugin before 6.2.8, when a pool is created with the options "Allow other answers", "Display other answers in the result list" and "Show results", it can lead to Stored Cross-Site Scripting issues as the 'Other' answer is not sanitised before being output in the page. The execution of the XSS payload depends on the 'Show results' option selected, which could be before or after sending the vote for example.	2021-07-12	4.3	CVE-2021-24454 MISC CONFIRM

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
admincolumns -- admin_columns	The Admin Columns WordPress plugin Free before 4.3.2 and Pro before 5.5.2 allowed to configure individual columns for tables. Each column had a type. The type "Custom Field" allowed to choose an arbitrary database column to display in the table. There was no escaping applied to the contents of "Custom Field" columns.	2021-07-12	3.5	CVE-2021-24365 CONFIRM MISC
blackcat-cms -- blackcat_cms	A stored cross site scripting (XSS) vulnerability in the 'Add Page' feature of BlackCat CMS 1.3.6 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	2021-07-09	3.5	CVE-2020-25877 MISC MISC
blackcat-cms -- blackcat_cms	A stored cross site scripting (XSS) vulnerability in the 'Admin-Tools' feature of BlackCat CMS 1.3.6 allows authenticated attackers to	2021-07-09	3.5	CVE-2020-25878

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execute arbitrary web scripts or HTML via crafted payloads entered into the 'Output Filters' and 'Droplets' modules.			MISC MISC
boldgrid -- w3_total_cache	The W3 Total Cache WordPress plugin before 2.1.3 did not sanitise or escape some of its CDN settings, allowing high privilege users to use JavaScript in them, which will be output in the page, leading to an authenticated Stored Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24427 MISC CONFIRM
codologic -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Manage Users' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Username' parameter.	2021-07-09	3.5	CVE-2020-25879 MISC MISC
codologic -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Smileys' feature of Codoforum v5.0.2 allows	2021-07-09	3.5	CVE-2020-25875

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Smiley Code' parameter.			MISC MISC
codologic -- codoforum	A stored cross site scripting (XSS) vulnerability in the 'Pages' feature of Codoforum v5.0.2 allows authenticated attackers to execute arbitrary web scripts or HTML via crafted payload entered into the 'Page Title' parameter.	2021-07-09	3.5	CVE-2020-25876 MISC MISC
cszcms -- csz_cms	A cross site scripting vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New Pages' field under the 'Pages Content' module.	2021-07-09	3.5	CVE-2020-25391 MISC
cszcms -- csz_cms	A cross site scripting (XSS) vulnerability in CSZ CMS 1.2.9 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'New	2021-07-09	3.5	CVE-2020-25392 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Article' field under the 'Article' plugin.			
dotcms -- dotcms	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/containers of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	2021-07-09	3.5	CVE-2021-35360 MISC
dotcms -- dotcms	A reflected cross site scripting (XSS) vulnerability in dotAdmin/#/c/links of dotCMS 21.05.1 allows attackers to execute arbitrary commands or HTML via a crafted payload.	2021-07-09	3.5	CVE-2021-35361 MISC
dotcms -- dotcms	A stored cross site scripting (XSS) vulnerability in dotAdmin/#/c/c_Images of dotCMS 21.05.1 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' and 'Filename' parameters.	2021-07-09	3.5	CVE-2021-35358 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
element-it -- http_commander	A Cross-site scripting (XSS) vulnerability in the "View in Browser" feature in Elements-IT HTTP Commander 5.3.3 allows remote authenticated users to inject arbitrary web script or HTML via a crafted SVG image.	2021-07-14	3.5	CVE-2021-33212 MISC MISC
emarketdegisn -- request_a_quote	The Request a Quote WordPress plugin before 2.3.4 did not sanitise and escape some of its quote fields when adding/editing a quote as admin, leading to Stored Cross-Site scripting issues when the quote is output in the 'All Quotes" table.	2021-07-12	3.5	CVE-2021-24420 CONFIRM
esri -- arcgis_server	A stored Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server Services Directory version 10.8.1 and below may allow a remote authenticated attacker to pass and store malicious strings in the ArcGIS Services Directory.	2021-07-11	3.5	CVE-2021-29105 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eyecix -- jobsearch_wp_job_board	The WP JobSearch WordPress plugin before 1.7.4 did not sanitise or escape multiple of its parameters from the my-resume page before outputting them in the page, allowing low privilege users to use JavaScript payloads in them and leading to a Stored Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24421 CONFIRM MISC
fetchdesigns -- sign-up_sheets	The Sign-up Sheets WordPress plugin before 1.0.14 did not sanitise or escape some of its fields when creating a new sheet, allowing high privilege users to add JavaScript in them, leading to a Stored Cross-Site Scripting issue. The payloads will be triggered when viewing the 'All Sheets' page in the admin dashboard	2021-07-12	3.5	CVE-2021-24440 CONFIRM
flowdroid_project -- flowdroid	FlowDroid is a data flow analysis tool. FlowDroid versions prior to 2.9.0 contained an XML external entity (XXE) vulnerability that allowed an attacker who had control over the source/sink definition file	2021-07-12	3.5	CVE-2021-32754 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in XML format to read files from external locations. In order for this to occur, the XML-based format for sources and sinks had to be used and the attacker had to able control the source/sink definition file. The vulnerability was patched in version 2.9.0. As a workaround, do not allow untrusted entities to control the source/sink definition file.			
google -- android	In generateFileInfo of BluetoothOppSendFileInfo.java, there is a possible way to share private files over Bluetooth due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-179910660	2021-07-14	1.9	CVE-2021-0604 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
halo -- halo	Cross Sie Scripting (XSS) vulnerability in Halo 0.4.3 via CommentAuthorUrl.	2021-07-12	3.5	CVE-2020-18982 MISC
huawei -- mate_20_firmware	There is a path traversal vulnerability in some Huawei products. The vulnerability is due to that the software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly validate the pathname. Successful exploit could allow the attacker to access a location that is outside of the restricted directory by a crafted filename. Affected product versions include:HUAWEI Mate 20 9.0.0.195(C01E195R2P1), 9.1.0.139(C00E133R3P1);HUAWEI Mate 20 Pro 9.0.0.187(C432E10R1P16), 9.0.0.188(C185E10R2P1), 9.0.0.245(C10E10R2P1),	2021-07-13	2.1	CVE-2021-22440 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	9.0.0.266(C432E10R1P16), 9.0.0.267(C636E10R2P1), 9.0.0.268(C635E12R1P16), 9.0.0.278(C185E10R2P1); Hima-L29C 9.0.0.105(C10E9R1P16), 9.0.0.105(C185E9R1P16), 9.0.0.105(C636E9R1P16); Laya-AL00EP 9.1.0.139(C786E133R3P1); OxfordS-AN00A 10.1.0.223(C00E210R5P1); Tony-AL00B 9.1.0.257(C00E222R2P1).			
huawei -- p30_firmware	The Bluetooth function of some Huawei smartphones has a DoS vulnerability. Attackers can install third-party apps to send specific broadcasts, causing the Bluetooth module to crash. This vulnerability is successfully exploited to cause the Bluetooth function to become abnormal. Affected product versions include: HUAWEI P30 10.0.0.195(C432E22R2P5), 10.0.0.200(C00E85R2P11), 10.0.0.200(C461E6R3P1),	2021-07-13	2.1	CVE-2021-22399 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	10.0.0.201(C10E7R5P1), 10.0.0.201(C185E4R7P1), 10.0.0.206(C605E19R1P3), 10.0.0.209(C636E6R3P4), 10.0.0.210(C635E3R2P4), and versions earlier than 10.1.0.165(C01E165R2P11).			
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 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: 195035.	2021-07-13	3.5	CVE-2021-20364 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 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	2021-07-13	3.5	CVE-2021-20368 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	within a trusted session. IBM X-Force ID: 195357.			
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 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: 195037.	2021-07-13	3.5	CVE-2021-20366 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 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: 195036.	2021-07-13	3.5	CVE-2021-20365 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 is vulnerable to cross-site	2021-07-13	3.5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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: 195034.			20363 CONFIRM XF
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 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: 195033.	2021-07-13	3.5	CVE-2021-20362 XF CONFIRM
ibm -- cloud_pak_for_applications	IBM Cloud Pak for Applications 4.3 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	2021-07-13	3.5	CVE-2021-20361 XF CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	within a trusted session. IBM X-Force ID: 195032.			
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored 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: 204262.	2021-07-12	3.5	CVE-2021-29804 XF CONFIRM
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored 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: 204263.	2021-07-12	3.5	CVE-2021-29805 CONFIRM XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 is vulnerable to stored 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: 204164.	2021-07-12	3.5	CVE-2021-29803 CONFIRM XF
ibm -- tivoli_netcool\/omnibus_gui	IBM Tivoli Netcool/OMNIbus_GUI 8.1.0 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: 204349.	2021-07-12	3.5	CVE-2021-29822 CONFIRM XF
icinga -- icinga	Icinga Web 2 is an open source monitoring web interface, framework and command-line interface. Between versions 2.3.0	2021-07-12	3.5	CVE-2021-32746 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	and 2.8.2, the `doc` module of Icinga Web 2 allows to view documentation directly in the UI. It must be enabled manually by an administrator and users need explicit access permission to use it. Then, by visiting a certain route, it is possible to gain access to arbitrary files readable by the web-server user. The issue has been fixed in the 2.9.0, 2.8.3, and 2.7.5 releases. As a workaround, an administrator may disable the `doc` module or revoke permission to use it from all users.			CONFIRM MISC MISC
kaseya -- vsa	Cross Site Scripting (XSS) exists in Kaseya VSA before 9.5.7.	2021-07-09	3.5	CVE-2021-30119 MISC
microsoft -- windows_10	Media Foundation Information Disclosure Vulnerability	2021-07-14	2.1	CVE-2021-33760 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
microsoft -- windows_10	Windows Remote Access Connection Manager Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-34454, CVE-2021-34457.	2021-07-14	2.1	CVE-2021-33763 MISC
microsoft -- windows_10	Windows Installer Spoofing Vulnerability	2021-07-14	2.1	CVE-2021-33765 MISC
microsoft -- windows_10	Windows InstallService Elevation of Privilege Vulnerability	2021-07-14	3.6	CVE-2021-31961 MISC
mozilo -- mozilocms	A stored cross site scripting (XSS) vulnerability in moziloCMS 2.0 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "Content" parameter.	2021-07-09	3.5	CVE-2020-25394 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nextcloud -- nextcloud_server	Nextcloud Server is a Nextcloud package that handles data storage. In versions priot to 19.0.13, 20.0.11, and 21.0.3, Nextcloud Server audit logging functionality wasn't properly logging events for the unsetting of a share expiration date. This event is supposed to be logged. This issue is patched in versions 19.0.13, 20.0.11, and 21.0.3.	2021-07-12	2.1	CVE-2021-32680 CONFIRM MISC MISC
pfsense -- pfsense	A Stored Cross-Site Scripting (XSS) vulnerability was found in status_filter_reload.php, a page in the pfSense software WebGUI, on Netgate pfSense version 2.4.4-p2 and earlier. The page did not encode output from the filter reload process, and a stored XSS was possible via the descr (description) parameter on NAT rules.	2021-07-12	3.5	CVE-2020-19201 MISC MISC MISC
plugin-planet -- prismatic	The Prismatic WordPress plugin before 2.8 does not sanitise or validate some of its shortcode	2021-07-12	3.5	CVE-2021-24408

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameters, allowing users with a role as low as Contributor to set Cross-Site payload in them. A post made by a contributor would still have to be approved by an admin to have the XSS trigger able in the frontend, however, higher privilege users, such as editor could exploit this without the need of approval, and even when the blog disallows the unfiltered_html capability.			CONFIRM
prothemedesign -- browser_screenshots	The Browser Screenshots WordPress plugin before 1.7.6 allowed authenticated users with a role as low as Contributor to perform Stored Cross-Site Scripting attacks as the image_class parameter of the browser-shot shortcode was not escaped.	2021-07-12	3.5	CVE-2021-24439 CONFIRM
publiccms -- publiccms	Cross Site Scripting (XSS) vulnerability in PublicCMS 4.0 to get an admin cookie when the Administrator reviews submit case.	2021-07-09	3.5	CVE-2020-21333 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- apq8009_firmware	Possible buffer over-read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1901 CONFIRM
qualcomm -- apq8009_firmware	Possible Buffer Over-read due to lack of validation of boundary checks when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1897 CONFIRM
qualcomm -- apq8009_firmware	Possible buffer over-read due to incorrect overflow check when loading splash image in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1898 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
qualcomm -- apq8009w_firmware	Possible buffer over read due to lack of length check while flashing meta images in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-07-13	2.1	CVE-2021-1899 CONFIRM
qualcomm -- aqt1000_firmware	Weak configuration in WLAN could cause forwarding of unencrypted packets from one client to another in Snapdragon Compute, Snapdragon Connectivity	2021-07-13	3.3	CVE-2021-1896 CONFIRM
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Users Access Groups' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	3.5	CVE-2020-35986 MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Entities List' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute	2021-07-09	3.5	CVE-2020-35987 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.			
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Users Alerts' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Title' parameter.	2021-07-09	3.5	CVE-2020-35984 MISC
rukovoditel -- rukovoditel	A stored cross site scripting (XSS) vulnerability in the 'Global Lists'' feature of Rukovoditel 2.7.2 allows authenticated attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the 'Name' parameter.	2021-07-09	3.5	CVE-2020-35985 MISC
sap -- lumira_server	SAP Lumira Server version 2.4 does not sufficiently encode user controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. This would allow an	2021-07-14	3.5	CVE-2021-33682 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attacker with basic level privileges to store a malicious script on SAP Lumira Server. The execution of the script content, by a victim registered on SAP Lumira Server, could compromise the confidentiality and integrity of SAP Lumira content.			
smooth_scroll_page_up\/down_buttons_project -- smooth_scroll_page_up\/down_buttons	The Smooth Scroll Page Up/Down Buttons WordPress plugin through 1.4 does not properly sanitise and validate its psb_positioning settings, allowing high privilege users such as admin to set an XSS payload in it, which will be executed in all pages of the blog	2021-07-12	3.5	CVE-2021-24418 CONFIRM MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows duplicating an existing security policy by leveraging access of a user having read-only access to security policies.	2021-07-13	2.9	CVE-2021-31224 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows modifying security policies by leveraging access of a user having read-only access to security policies.	2021-07-13	2.3	CVE-2021-31220 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows reading some parts of a security policy by leveraging access to a computer having the administration console installed.	2021-07-13	2.9	CVE-2021-31223 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows updating some parts of a security policy by leveraging access to a computer having the administration console installed.	2021-07-13	2.9	CVE-2021-31222 MISC MISC
stormshield -- endpoint_security	SES Evolution before 2.1.0 allows deleting some parts of a security policy by leveraging access to a computer having the administration console installed.	2021-07-13	2.9	CVE-2021-31221 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
web-dorado -- backup-wd	The Backup by 10Web â€“ Backup and Restore Plugin WordPress plugin through 1.0.20 does not sanitise or escape the tab parameter before outputting it back in the page, leading to a reflected Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24426 MISC CONFIRM
webfactoryltd -- wp_reset	The WP Reset â€“ Most Advanced WordPress Reset Tool WordPress plugin before 1.90 did not sanitise or escape its extra_data parameter when creating a snapshot via the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue	2021-07-12	3.5	CVE-2021-24424 CONFIRM MISC
wp_youtube_lyte_project -- wp_youtube_lyte	The WP YouTube Lyte WordPress plugin before 1.7.16 did not sanitise or escape its lyte_yt_api_key and lyte_notification settings before outputting them back in the page, allowing high privilege users to set XSS payload on them and leading to stored Cross-Site Scripting issues.	2021-07-12	3.5	CVE-2021-24419 CONFIRM MISC