Vulnerability Summary for the Week of April 5, 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**
apple -- ipad_os	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution.	2021-04-02	7.5	CVE-2021-1794 MISC
apple -- ipad_os	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS	2021-04-02	7.5	CVE-2021-1796 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	14.4. A remote attacker may be able to cause arbitrary code execution.			
apple -- ipad_os	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.	2021-04-02	7.5	CVE-2021-1818 MISC MISC MISC MISC
apple -- ipad_os	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution.	2021-04-02	7.5	CVE-2021-1795 MISC
apple -- ipados	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.0.1, tvOS 14.0, macOS Big Sur 11.1, Security Update 2020-001 Catalina,	2021-04-02	9.3	CVE-2020-9975 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Security Update 2020-007 Mojave, watchOS 7.0, iOS 14.0 and iPadOS 14.0. An application may be able to execute arbitrary code with kernel privileges.			MISC MISC MISC
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to heap corruption.	2021-04-02	9.3	CVE-2021-1767 MISC MISC
apple -- ipados	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	2021-04-02	9.3	CVE-2021-1763 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ipados	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution.	2021-04-02	9.3	CVE-2021-1758 MISC MISC MISC MISC
apple -- ipados	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. An application may be able to execute arbitrary code with kernel privileges.	2021-04-02	9.3	CVE-2021-1750 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS	2021-04-02	7.1	CVE-2021-1791 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	14.4 and iPadOS 14.4. A malicious application may be able to disclose kernel memory.			
apple -- ipados	Multiple memory corruption issues were addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, tvOS 14.0, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, watchOS 7.0, iOS 14.0 and iPadOS 14.0. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	2021-04-02	9.3	CVE-2020-9967 MISC MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	9.3	CVE-2021-1759 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. An application may be able to execute arbitrary code with kernel privileges.	2021-04-02	9.3	CVE-2020-27947 MISC
apple -- mac_os_x	A race condition was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. An application may be able to execute arbitrary code with kernel privileges.	2021-04-02	9.3	CVE-2020-27921 MISC MISC
apple -- mac_os_x	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. A malicious application may be able to	2021-04-02	9.3	CVE-2020-27915 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	execute arbitrary code with system privileges.			
apple -- mac_os_x	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. A malicious application may be able to execute arbitrary code with system privileges.	2021-04-02	9.3	CVE-2020-27914 MISC MISC
apple -- mac_os_x	A logic error in kext loading was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. An application may be able to execute arbitrary code with system privileges.	2021-04-02	9.3	CVE-2021-1779 MISC
apple -- mac_os_x	An out-of-bounds write was addressed with improved input validation. This	2021-04-02	9.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue is fixed in macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, macOS Mojave 10.14.6 Security Update 2021-002. An application may be able to execute arbitrary code with kernel privileges.			1805 MISC
apple -- mac_os_x	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A malicious application may be able to execute arbitrary code with system privileges.	2021-04-02	9.3	CVE-2020-29612 MISC
apple -- mac_os_x	A race condition was addressed with additional validation. This issue is fixed in macOS Big Sur 11.2.1, macOS Catalina 10.15.7 Supplemental Update, macOS Mojave 10.14.6 Security Update 2021-002. An application may be able to execute arbitrary code with kernel privileges.	2021-04-02	7.6	CVE-2021-1806 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. An application may be able to execute arbitrary code with kernel privileges.	2021-04-02	9.3	CVE-2020-10015 MISC MISC
apple -- mac_os_x	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. An application may be able to execute arbitrary code with kernel privileges.	2021-04-02	9.3	CVE-2020-27897 MISC MISC
apple -- macos	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. An	2021-04-02	9.3	CVE-2020-27907 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application may be able to execute arbitrary code with kernel privileges.			
apple -- maos	A validation issue was addressed with improved logic. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. An application may be able to execute arbitrary code with kernel privileges.	2021-04-02	9.3	CVE-2020-27941 MISC
cohesity -- cohesity_dataplatform	Undocumented Default Cryptographic Key Vulnerability in Cohesity DataPlatform version 6.3 prior 6.3.1g, 6.4 up to 6.4.1c and 6.5.1 through 6.5.1b. The ssh key can provide an attacker access to the linux system in the affected version.	2021-04-02	7.5	CVE-2021-28123 CONFIRM
coreftp -- core_ftp	Buffer overflow vulnerability in Core FTP Server v1.2 Build 583, via a crafted username.	2021-04-05	7.5	CVE-2020-19596 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
deltaflow_project -- deltaflow	The Vangene deltaFlow E-platform does not take properly protective measures. Attackers can obtain privileged permissions remotely by tampering with users' data in the Cookie.	2021-04-06	7.5	CVE-2021-28171 MISC MISC
deltaflow_project -- deltaflow	The file upload function of Vangene deltaFlow E-platform does not perform access controlled properly. Remote attackers can upload and execute arbitrary files without login.	2021-04-06	7.5	CVE-2021-28173 MISC MISC
dlink -- dir-846_firmware	HNAP1/control/SetMasterWLanSettings.php in D-Link D-Link Router DIR-846 DIR-846 A1_100.26 allows remote attackers to execute arbitrary commands via shell metacharacters in the ssid0 or ssid1 parameter.	2021-04-02	10	CVE-2020-27600 MISC MISC MISC
dlink -- dir-878_firmware	An issue was discovered in prog.cgi on D-Link DIR-878 1.30B08 devices. Because strcat is misused, there is a	2021-04-02	7.5	CVE-2021-30072

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	stack-based buffer overflow that does not require authentication.			MISC MISC
dmasoftlab -- dma_radius_manager	DMA Softlab Radius Manager 4.4.0 assigns the same session cookie to every admin session. The cookie is valid when the admin is logged in, but is invalid (temporarily) during times when the admin is logged out. In other words, the cookie is functionally equivalent to a static password, and thus provides permanent access if stolen.	2021-04-02	7.5	CVE-2021-29012 MISC MISC
emlog -- emlog	Vulnerability in emlog v6.0.0 allows user to upload webshells via zip plugin module.	2021-04-02	7.5	CVE-2020-21585 MISC MISC
htmldoc_project -- htmldoc	Integer overflow in the htmldoc 1.9.11 and before may allow attackers to execute arbitrary code and cause a denial of service that is similar to CVE-2017-9181.	2021-04-05	7.5	CVE-2021-20308 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
latrix_project -- latrix	An issue was discovered in LATRIX 0.6.0. SQL injection in the txtaccesscode parameter of inandout.php leads to information disclosure and code execution.	2021-04-02	7.5	CVE-2021-30000 MISC MISC
libpano13_project -- libpano13	Format string vulnerability in panoFileOutputNamesCreate() in libpano13 2.9.20~rc2+dfsg-3 and earlier can lead to read and write arbitrary memory values.	2021-04-05	7.5	CVE-2021-20307 MISC MISC
luvion -- grand_elite_3_connect_firmware	An issue was discovered in Luvion Grand Elite 3 Connect through 2020-02-25. Authentication to the device is based on a username and password. The root credentials are the same across all devices of this model.	2021-04-02	8.3	CVE-2020-11925 MISC
magpierss_project -- magpierss	Because of a incorrect escaped exec command in MagpieRSS in 0.72 in the /extlib/Snoopy.class.inc file, it is possible to add a extra command to the curl binary. This creates an issue on the	2021-04-02	7.5	CVE-2021-28940 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	/scripts/magpie_debug.php and /scripts/magpie_simple.php page that if you send a specific https url in the RSS URL field, you are able to execute arbitrary commands.			
nettle_project -- nettle	A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalers, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability.	2021-04-05	7.5	CVE-2021-20305 MISC
ocproducts -- composr	Composr 10.0.36 allows upload and execution of PHP files.	2021-04-06	7.5	CVE-2021-30149 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
okta -- access_gateway	A command injection vulnerability in the cookieDomain and relayDomain parameters of Okta Access Gateway before 2020.9.3 allows attackers (with admin access to the Okta Access Gateway UI) to execute OS commands as a privileged system account.	2021-04-02	9	CVE-2021-28113 CONFIRM
openiam -- openiam	OpenIAM before 4.2.0.3 allows remote attackers to execute arbitrary code via Groovy Script.	2021-04-06	7.5	CVE-2020-13420 MISC
openiam -- openiam	OpenIAM before 4.2.0.3 has Incorrect Access Control for the Create User, Modify User Permissions, and Password Reset actions.	2021-04-06	7.5	CVE-2020-13421 MISC
posimyth -- the_plus_addons_for_elementor	The Plus Addons for Elementor Page Builder WordPress plugin before 4.1.7 was being actively exploited to by malicious actors to bypass authentication, allowing unauthenticated users to log in as any	2021-04-05	7.5	CVE-2021-24175 MISC CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	user (including admin) by just providing the related username, as well as create accounts with arbitrary roles, such as admin. These issues can be exploited even if registration is disabled, and the Login widget is not active.			RM MISC
redmine -- redmine	Redmine before 4.0.8 and 4.1.x before 4.1.2 allows attackers to bypass the add_issue_notes permission requirement by leveraging the Issues API.	2021-04-06	7.5	CVE-2021-30164 MISC
riot-os -- riot	RIOT-OS 2021.01 contains a buffer overflow vulnerability in sys/net/gnrc/routing/rpl/gnrc_rpl_validation.c through the gnrc_rpl_validation_options() function.	2021-04-06	7.5	CVE-2021-27697 MISC
riot-os -- riot	RIOT-OS 2021.01 contains a buffer overflow vulnerability in /sys/net/gnrc/routing/rpl/gnrc_rpl_control_messages.c through the _parse_options() function.	2021-04-06	7.5	CVE-2021-27698 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
riot-os -- riot	RIOT-OS 2020.01 contains a buffer overflow vulnerability in /sys/net/gnrc/routing/rpl/gnrc_rpl_control_messages.c.	2021-04-06	7.5	CVE-2021-27357 MISC
sannce -- smart_hd_wifi_security_camera_ean_2_950004_595317_firmware	An issue was discovered on Sannce Smart HD Wifi Security Camera EAN 2 950004 595317 devices. A crash and reboot can be triggered by crafted IP traffic, as demonstrated by the Nikto vulnerability scanner. For example, sending the 111111 string to UDP port 20188 causes a reboot. To deny service for a long time period, the crafted IP traffic may be sent periodically.	2021-04-02	7.8	CVE-2019-20463 MISC
sannce -- smart_hd_wifi_security_camera_ean_2_950004_595317_firmware	An issue was discovered on Sannce Smart HD Wifi Security Camera EAN 2 950004 595317 devices. A local attacker with the "default" account is capable of reading the /etc/passwd file, which contains a weakly hashed root password. By taking this hash and cracking it, the attacker can obtain root rights on the device.	2021-04-02	7.2	CVE-2019-20466 MISC

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
algolplus -- advanced_order_export	This Advanced Order Export For WooCommerce WordPress plugin before 3.1.8 helps you to easily export WooCommerce order data. The tab parameter in the Admin Panel is vulnerable to reflected XSS.	2021-04-05	4.3	CVE-2021-24169 CONFIRM
apache -- cxf	CXF supports (via JwtRequestCodeFilter) passing OAuth 2 parameters via a JWT token as opposed to query parameters (see: The OAuth 2.0 Authorization Framework: JWT Secured Authorization Request (JAR)). Instead of sending a JWT token as a "request" parameter, the spec also supports specifying a URI from which to retrieve a JWT token from via the "request_uri" parameter. CXF was not validating the "request_uri" parameter (apart from ensuring it uses "https) and was making a REST request to the parameter in the	2021-04-02	5	CVE-2021-22696 MLIST CONFIRM MLIST MLIST MLIST MLIST

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	request to retrieve a token. This means that CXF was vulnerable to DDos attacks on the authorization server, as specified in section 10.4.1 of the spec. This issue affects Apache CXF versions prior to 3.4.3; Apache CXF versions prior to 3.3.10.			
apple -- icloud	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.3, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, iCloud for Windows 12.0, watchOS 7.2. Processing a maliciously crafted image may lead to heap corruption.	2021-04-02	6.8	CVE-2020-29617 MISC MISC MISC MISC MISC
apple -- icloud	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.3, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, iCloud for Windows 12.0, watchOS 7.2.	2021-04-02	6.8	CVE-2020-29619 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Processing a maliciously crafted image may lead to heap corruption.			MISC MISC
apple -- icloud	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.3, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, iCloud for Windows 12.0, watchOS 7.2. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-29618 MISC MISC MISC MISC MISC
apple -- icloud	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, iCloud for Windows 7.20, macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra. Processing maliciously crafted XML may lead to an unexpected application termination or arbitrary code execution.	2021-04-02	6.8	CVE-2020-9926 MISC MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- icloud	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 14.3, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, iCloud for Windows 12.0, watchOS 7.2. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-29611 MISC MISC MISC MISC MISC
apple -- icloud	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, iCloud for Windows 7.20, watchOS 6.2.8, tvOS 13.4.8, macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-27933 MISC MISC MISC MISC MISC
apple -- ipad_os	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1,	2021-04-02	6.8	CVE-2020-27908

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, watchOS 7.1, tvOS 14.2. Processing a maliciously crafted audio file may lead to arbitrary code execution.			MISC MISC MISC MISC MISC
apple -- ipad_os	This issue was addressed by improved management of object lifetimes. This issue is fixed in iOS 12.5.2, iOS 14.4.2 and iPadOS 14.4.2, watchOS 7.3.3. Processing maliciously crafted web content may lead to universal cross site scripting. Apple is aware of a report that this issue may have been actively exploited..	2021-04-02	4.3	CVE-2021-1879 MISC MISC MISC
apple -- ipad_os	A memory corruption issue existed in the processing of font files. This issue was addressed with improved input validation. This issue is fixed in watchOS 7.2, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS	2021-04-02	6.8	CVE-2020-27944 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	14.3 and iPadOS 14.3, tvOS 14.3. Processing a maliciously crafted font file may lead to arbitrary code execution.			
apple -- ipad_os	A memory corruption issue existed in the processing of font files. This issue was addressed with improved input validation. This issue is fixed in tvOS 14.3, iOS 14.3 and iPadOS 14.3, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, watchOS 7.2. Processing a maliciously crafted font file may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-27943 MISC MISC MISC MISC
apple -- ipad_os	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Big Sur 11.0.1, watchOS 7.1, tvOS 14.2. A local attacker may be able to elevate their privileges.	2021-04-02	4.6	CVE-2020-27899 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ipad_os	Multiple issues were addressed with improved logic. This issue is fixed in iOS 14.2 and iPadOS 14.2, macOS Big Sur 11.0.1, watchOS 7.1, tvOS 14.2. A sandboxed process may be able to circumvent sandbox restrictions.	2021-04-02	4.3	CVE-2020-27935 MISC MISC MISC MISC
apple -- ipados	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1789 FEDORA FEDORA MISC MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina,	2021-04-02	6.8	CVE-2021-1792 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause arbitrary code execution.			MISC MISC MISC
apple -- ipados	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.3 and iPadOS 14.3. An enterprise application installation prompt may display the wrong domain.	2021-04-02	4.3	CVE-2020-29613 MISC
apple -- ipados	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4, Safari 14.0.3. Processing maliciously crafted web content may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1788 FEDORA MISC MISC MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved input validation. This	2021-04-02	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.			1785 MISC MISC MISC MISC
apple -- ipados	An access issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1783 MISC MISC MISC MISC
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a	2021-04-02	6.8	CVE-2021-1777 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	maliciously crafted image may lead to arbitrary code execution.			
apple -- ipados	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted font file may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1776 MISC MISC MISC MISC
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1774 MISC MISC MISC MISC
apple -- ipados	A use after free issue was addressed with improved memory management.	2021-04-02	5	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A remote attacker may be able to cause a denial of service.			1764 MISC MISC MISC MISC
apple -- ipados	A race condition was addressed with improved locking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious application may be able to elevate privileges. Apple is aware of a report that this issue may have been actively exploited..	2021-04-02	6.9	CVE-2021-1782 MISC MISC MISC MISC MISC
apple -- ipados	A privacy issue existed in the handling of Contact cards. This was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS	2021-04-02	4.3	CVE-2021-1781 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	14.4 and iPadOS 14.4. A malicious application may be able to leak sensitive user information.			
apple -- ipados	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted USD file may lead to unexpected application termination or arbitrary code execution.	2021-04-02	6.8	CVE-2021-1768 MISC MISC
apple -- ipados	An out-of-bounds read issue existed in the curl. This issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service.	2021-04-02	4.3	CVE-2021-1778 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ipados	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service.	2021-04-02	4.3	CVE-2021-1773 MISC MISC MISC MISC
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to a denial of service.	2021-04-02	4.3	CVE-2021-1766 MISC MISC MISC MISC
apple -- ipados	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A	2021-04-02	4.3	CVE-2021-1760 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	malicious application could execute arbitrary code leading to compromise of user information.			
apple -- ipados	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 14.4 and iPadOS 14.4. An attacker in a privileged position may be able to perform a denial of service attack.	2021-04-02	4.9	CVE-2021-1780 MISC
apple -- ipados	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local user may be able to create or modify system files.	2021-04-02	4.9	CVE-2021-1786 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina,	2021-04-02	4.6	CVE-2021-1757 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges.			MISC MISC MISC
apple -- ipados	Multiple issues were addressed with improved logic. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A local attacker may be able to elevate their privileges.	2021-04-02	4.6	CVE-2021-1787 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted font may result in the disclosure of process memory.	2021-04-02	4.3	CVE-2020-29639 MISC
apple -- ipados	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 7.2, macOS	2021-04-02	4.3	CVE-2020-29615

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, tvOS 14.3. Processing a maliciously crafted image may lead to a denial of service.			MISC MISC MISC MISC
apple -- ipados	An information disclosure issue was addressed with improved state management. This issue is fixed in watchOS 7.2, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, tvOS 14.3. Processing a maliciously crafted font may result in the disclosure of process memory.	2021-04-02	4.3	CVE-2020-27946 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, tvOS 14.3, macOS Big Sur 11.1, Security Update 2020-001 Catalina,	2021-04-02	4.3	CVE-2020-29608 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, watchOS 7.2. A remote attacker may be able to leak memory.			MISC MISC
apple -- ipados	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted text file may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1772 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 7.2, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, tvOS 14.3. Processing a maliciously crafted audio file may disclose restricted memory.	2021-04-02	4.3	CVE-2020-29610 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1754 MISC MISC MISC MISC
apple -- ipados	A logic issue was addressed with improved validation. This issue is fixed in watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0, macOS Big Sur 11.0.1. A malicious application may be able to elevate privileges.	2021-04-02	6.8	CVE-2020-9971 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in watchOS 7.2, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, tvOS 14.3. Processing a	2021-04-02	6.8	CVE-2020-27948 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	maliciously crafted audio file may lead to arbitrary code execution.			
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in watchOS 6.3, iOS 12.5, iOS 14.3 and iPadOS 14.3, watchOS 7.2. Unauthorized code execution may lead to an authentication policy violation.	2021-04-02	6.8	CVE-2020-27951 MISC MISC MISC MISC
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, tvOS 14.3. Processing a maliciously crafted file may lead to heap corruption.	2021-04-02	6.8	CVE-2020-29614 MISC MISC MISC MISC
apple -- ipados	A memory corruption issue existed in the processing of font files. This issue	2021-04-02	6.8	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	was addressed with improved input validation. This issue is fixed in watchOS 7.2, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, tvOS 14.3. Processing a maliciously crafted font file may lead to arbitrary code execution.			29624 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in watchOS 7.0, tvOS 14.0, iOS 14.0 and iPadOS 14.0, macOS Big Sur 11.0.1. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-9955 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1, tvOS 14.0, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, watchOS 7.0, iOS 14.0 and iPadOS	2021-04-02	6.8	CVE-2020-9956 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	14.0. Processing a maliciously crafted font file may lead to arbitrary code execution.			MISC MISC
apple -- ipados	A validation issue was addressed with improved input sanitization. This issue is fixed in tvOS 14.4, watchOS 7.3, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted URL may lead to arbitrary javascript code execution.	2021-04-02	6.8	CVE-2021-1748 MISC MISC MISC
apple -- ipados	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.0.1, tvOS 14.0, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, watchOS 7.0, iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-9962 MISC MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.0.1,	2021-04-02	6.8	CVE-2020-9960

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	tvOS 14.0, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, watchOS 7.0, iOS 14.0 and iPadOS 14.0. Processing a maliciously crafted audio file may lead to arbitrary code execution.			MISC MISC MISC MISC MISC
apple -- ipados	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1741 MISC MISC MISC MISC
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a	2021-04-02	6.8	CVE-2021-1742 MISC MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	maliciously crafted image may lead to arbitrary code execution.			
apple -- ipados	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1743 MISC MISC MISC MISC
apple -- ipados	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1746 MISC MISC MISC MISC
apple -- ipados	An out-of-bounds write was addressed with improved input validation. This	2021-04-02	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. Processing maliciously crafted web content may lead to code execution.			1747 MISC MISC MISC MISC
apple -- mac_os_x	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-29625 MISC
apple -- mac_os_x	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, macOS Big Sur 11.0.1. A malicious application may be able to access private information.	2021-04-02	4.3	CVE-2020-27937 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1738 MISC
apple -- mac_os_x	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, watchOS 7.1, tvOS 14.2. Processing maliciously crafted web content may lead to code execution.	2021-04-02	6.8	CVE-2020-27920 MISC MISC MISC MISC MISC
apple -- mac_os_x	This issue was addressed with improved entitlements. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A malicious	2021-04-02	6.8	CVE-2020-29620 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	application may be able to elevate privileges.			
apple -- mac_os_x	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, watchOS 7.1, tvOS 14.2. Processing a maliciously crafted font file may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-27922 MISC MISC MISC MISC MISC
apple -- mac_os_x	A memory corruption issue was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-29616 MISC
apple -- mac_os_x	This issue was addressed by removing the vulnerable code. This issue is fixed	2021-04-02	6.8	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted font may lead to arbitrary code execution.			1775 MISC
apple -- mac_os_x	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. Processing a maliciously crafted font file may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-27952 MISC MISC
apple -- mac_os_x	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Maliciously crafted web content may violate iframe sandboxing policy.	2021-04-02	4.3	CVE-2021-1765 FEDORA FEDORA MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, macOS Big Sur 11.0.1. Processing maliciously crafted web content may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-27945 MISC MISC
apple -- mac_os_x	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1736 MISC
apple -- mac_os_x	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Mounting a maliciously crafted Samba network share may lead to arbitrary code execution.	2021-04-02	4.6	CVE-2021-1751 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A malicious application may be able to elevate privileges.	2021-04-02	6.8	CVE-2020-27938 MISC MISC
apple -- mac_os_x	A memory corruption issue existed in the processing of font files. This issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1, watchOS 7.0, tvOS 14.0. Processing a maliciously crafted font file may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-27931 MISC MISC MISC MISC MISC
apple -- mac_os_x	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security	2021-04-02	4.6	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Update 2021-001 Catalina, Security Update 2021-001 Mojave. A local attacker may be able to elevate their privileges.			1802 MISC
apple -- mac_os_x	An authentication issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. An attacker in a privileged network position may be able to bypass authentication policy.	2021-04-02	6.5	CVE-2020-29633 MISC MISC
apple -- mac_os_x	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Catalina 10.15.6, Security Update 2020-004 Mojave, Security Update 2020-004 High Sierra. A local user may be able to cause unexpected system termination or read kernel memory.	2021-04-02	6.6	CVE-2020-9930 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A local user may be able to cause unexpected system termination or read kernel memory.	2021-04-02	6.6	CVE-2020-27936 MISC
apple -- mac_os_x	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A malicious application may cause unexpected changes in memory belonging to processes traced by DTrace.	2021-04-02	4.3	CVE-2020-27949 MISC
apple -- mac_os_x	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave,	2021-04-02	6.8	CVE-2020-27919 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	macOS Big Sur 11.0.1. Processing a maliciously crafted image may lead to arbitrary code execution.			
apple -- mac_os_x	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1737 MISC
apple -- mac_os_x	An input validation issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A malicious application may be able to read restricted memory.	2021-04-02	4.3	CVE-2020-10001 MISC
apple -- mac_os_x	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina,	2021-04-02	6.8	CVE-2020-27924 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Security Update 2020-007 Mojave, macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, watchOS 7.1, tvOS 14.2. Processing a maliciously crafted image may lead to arbitrary code execution.			MISC MISC MISC MISC
apple -- mac_os_x	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1, iOS 14.2 and iPadOS 14.2, watchOS 7.1, tvOS 14.2. Processing a maliciously crafted image may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2020-27923 MISC MISC MISC MISC MISC
apple -- macos	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.0.1. A malicious application with root privileges may be able to access private information.	2021-04-02	4.3	CVE-2020-10008 MISC
apple -- macos	This issue was addressed with improved checks. This issue is fixed in macOS	2021-04-02	6.8	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. Processing a maliciously crafted image may lead to arbitrary code execution.			27939 MISC
apple -- macos	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, macOS Big Sur 11.0.1. A sandboxed process may be able to circumvent sandbox restrictions.	2021-04-02	4.3	CVE-2020-27901 MISC MISC
apple -- macos	The issue was addressed with improved permissions logic. This issue is fixed in macOS Big Sur 11.0.1. A local application may be able to enumerate the user's iCloud documents.	2021-04-02	4.3	CVE-2021-1803 MISC
apple -- macos	An issue existed in screen sharing. This issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. A user with	2021-04-02	4	CVE-2020-27893 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	screen sharing access may be able to view another user's screen.			
apple -- macos_server	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Server 5.11. Processing a maliciously crafted URL may lead to an open redirect or cross site scripting.	2021-04-02	5.8	CVE-2020-9995 MISC
apple -- safari	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 14.4.1 and iPadOS 14.4.1, Safari 14.0.3 (v. 14610.4.3.1.7 and 15610.4.3.1.7), watchOS 7.3.2, macOS Big Sur 11.2.3. Processing maliciously crafted web content may lead to arbitrary code execution.	2021-04-02	6.8	CVE-2021-1844 FEDORA MISC MISC MISC MISC
apple -- xcode	A path handling issue was addressed with improved validation. This issue is fixed in Xcode 12.4. A malicious application may be able to access	2021-04-02	4.3	CVE-2021-1800 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	arbitrary files on the host device while running an app that uses on-demand resources with Xcode.			
asus -- z10pr-d16_firmware	The Radius configuration function in ASUS BMC's firmware Web management page does not verify the string length entered by users, resulting in a Buffer overflow vulnerability. As obtaining the privileged permission, remote attackers use the leakage to abnormally terminate the Web service.	2021-04-06	4	CVE-2021-28175 CONFIRM CONFIRM CONFIRM
cohesity -- cohesity_dataplatform	A man-in-the-middle vulnerability in Cohesity DataPlatform support channel in version 6.3 up to 6.3.1g, 6.4 up to 6.4.1c and 6.5.1 through 6.5.1b. Missing server authentication in impacted versions can allow an attacker to Man-in-the-middle (MITM) support channel UI session to Cohesity DataPlatform cluster.	2021-04-02	4.3	CVE-2021-28124 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
contribsys -- sidekiq	Sidekiq through 5.1.3 and 6.x through 6.2.0 allows XSS via the queue name of the live-poll feature when Internet Explorer is used.	2021-04-06	4.3	CVE-2021-30151 MISC
coreftp -- core_ftp	Buffer overflow vulnerability in Core FTP Server v2 Build 697, via a crafted username.	2021-04-05	5	CVE-2020-19595 MISC
cozmoslabs -- user_profile_picture	The REST API endpoint get_users in the User Profile Picture WordPress plugin before 2.5.0 returned more information than was required for its functionality to users with the upload_files capability. This included password hashes, hashed user activation keys, usernames, emails, and other less sensitive information.	2021-04-05	5	CVE-2021-24170 CONFIRM MISC
daifukuya -- kagemai	Cross-site scripting vulnerability in Kagemai 0.8.8 allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-04-07	4.3	CVE-2021-20685 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
daifukuya -- kagemai	Cross-site request forgery (CSRF) vulnerability in Kagemai 0.8.8 allows remote attackers to hijack the authentication of administrators via unspecified vectors.	2021-04-07	6.8	CVE-2021-20687 MISC
daifukuya -- kagemai	Cross-site scripting vulnerability in Kagemai 0.8.8 allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-04-07	4.3	CVE-2021-20686 MISC
database-backups_project -- database-backups	The Database Backups WordPress plugin through 1.2.2.6 does not have CSRF checks, allowing attackers to make a logged in user unwanted actions, such as generate backups of the database, change the plugin's settings and delete backups.	2021-04-05	5.8	CVE-2021-24174 CONFIRM
dell -- system_update	Dell System Update (DSU) 1.9 and earlier versions contain a denial of service vulnerability. A local authenticated malicious user with low privileges may potentially exploit this	2021-04-02	4.9	CVE-2021-21529 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	vulnerability to cause the system to run out of memory by running multiple instances of the vulnerable application.			
dell -- wyse_management_suite	Wyse Management Suite versions up to 3.2 contains a vulnerability wherein a malicious authenticated user can cause a denial of service in the job status retrieval page, also affecting other users that would have normally access to the same subset of job details	2021-04-02	4	CVE-2021-21533 MISC
deltaflow_project -- deltaflow	There is a Path Traversal vulnerability in the file download function of Vangene deltaFlow E-platform. Remote attackers can access credential data with this leakage.	2021-04-06	5	CVE-2021-28172 MISC MISC
dmasoftlab -- dma_radius_manager	DMA Softlab Radius Manager 4.4.0 is affected by Cross Site Scripting (XSS) via the description, name, or address field (under admin.php).	2021-04-02	4.3	CVE-2021-29011 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
docsifyjs -- docsify	docsify 4.12.1 is affected by Cross Site Scripting (XSS) because the search component does not appropriately encode Code Blocks and mishandles the " character.	2021-04-02	4.3	CVE-2021-30074 MISC
eng -- knowage	Knowage Suite before 7.4 is vulnerable to cross-site scripting (XSS). An attacker can inject arbitrary external script in '/knowagecockpitengine/api/1.0/pages/execute' via the 'SBI_HOST' parameter.	2021-04-05	4.3	CVE-2021-30058 MISC
eng -- knowage	A SQL injection vulnerability in Knowage Suite version 7.1 exists in the documentexecution/url analytics driver component via the 'par_year' parameter when running a report.	2021-04-05	6.5	CVE-2021-30055 MISC
expresstech -- responsive_menu	In the Reponsive Menu (free and Pro) WordPress plugins before 4.0.4, subscribers could upload zip archives containing malicious PHP files that would get extracted to the /rmp-menu/	2021-04-05	6.5	CVE-2021-24160 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	directory. These files could then be accessed via the front end of the site to trigger remote code execution and ultimately allow an attacker to execute commands to further infect a WordPress site.			RM MISC
expresstech -- responsive_menu	In the Reponsive Menu (free and Pro) WordPress plugins before 4.0.4, attackers could craft a request and trick an administrator into importing all new settings. These settings could be modified to include malicious JavaScript, therefore allowing an attacker to inject payloads that could aid in further infection of the site.	2021-04-05	6.8	CVE-2021-24162 CONFIRM MISC
expresstech -- responsive_menu	In the Reponsive Menu (free and Pro) WordPress plugins before 4.0.4, attackers could craft a request and trick an administrator into uploading a zip archive containing malicious PHP files. The attacker could then access those files to achieve remote code execution and further infect the targeted site.	2021-04-05	6.8	CVE-2021-24161 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
froala -- froala_editor	Froala Editor 3.2.6 is affected by Cross Site Scripting (XSS). Under certain conditions, a base64 crafted string leads to persistent Cross-site scripting (XSS) vulnerability within the hyperlink creation module.	2021-04-05	4.3	CVE-2021-30109 MISC MISC
github -- enterprise_server	An improper access control vulnerability was identified in GitHub Enterprise Server that allowed access tokens generated from a GitHub App's web authentication flow to read private repository metadata via the REST API without having been granted the appropriate permissions. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the application through the web authentication flow. The private repository metadata returned would be limited to repositories owned by the user the token identifies. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.0.4 and was fixed in versions 3.0.4, 2.22.10,	2021-04-02	4.3	CVE-2021-22865 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	2.21.18. This vulnerability was reported via the GitHub Bug Bounty program.			
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting with 12.6. Under a special condition it was possible to access data of an internal repository through a public project fork as an anonymous user.	2021-04-02	4.3	CVE-2021-22200 CONFIRM MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting with 13.7.9. A specially crafted Wiki page allowed attackers to read arbitrary files on the server.	2021-04-02	5	CVE-2021-22203 CONFIRM MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all previous versions. If the victim is an admin, it was possible to issue a CSRF in System hooks through the API.	2021-04-02	4.3	CVE-2021-22202 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.6 where an infinite loop exist when an authenticated user with specific rights access a MR having source and target branch pointing to each other	2021-04-02	4	CVE-2021-22197 CONFIRM MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions from 13.8 and above allowing an authenticated user to delete incident metric images of public projects.	2021-04-02	4	CVE-2021-22198 CONFIRM MISC MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.9. A specially crafted import file could read files on the server.	2021-04-02	4	CVE-2021-22201 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				MISC MISC
glpi-project -- dashboard	The Dashboard plugin through 1.0.2 for GLPI allows remote low-privileged users to bypass access control on viewing information about the last ten events, the connected users, and the users in the tech category. For example, plugins/dashboard/front/main2.php can be used.	2021-04-06	4	CVE-2021-30144 MISC MISC
jamf -- jamf	Jamf Pro before 10.28.0 allows XSS related to inventory history, aka PI-009376.	2021-04-02	4.3	CVE-2021-30125 MISC
lightmeter -- controlcenter	Lightmeter ControlCenter 1.1.0 through 1.5.x before 1.5.1 allows anyone who knows the URL of a publicly available Lightmeter instance to access application settings, possibly including an SMTP password and a Slack access token, via a settings HTTP query.	2021-04-02	6.4	CVE-2021-30126 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
magnolia-cms -- magnolia_cms	Magnolia CMS contains a stored cross-site scripting (XSS) vulnerability in the /magnoliaPublic/travel/members/login.html mgnlUserId parameter.	2021-04-02	4.3	CVE-2021-25894 MISC MISC MISC
magpierss_project -- magpierss	Because of no validation on a curl command in MagpieRSS 0.72 in the /extlib/Snoopy.class.inc file, when you send a request to the /scripts/magpie_debug.php or /scripts/magpie_simple.php page, it's possible to request any internal page if you use a https request.	2021-04-02	5	CVE-2021-28941 MISC MISC
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. Blocked users are unable to use Special:ResetTokens. This has security relevance because a blocked user might have accidentally shared a token, or might know that a token has been compromised, and yet is not able	2021-04-06	5	CVE-2021-30158 MISC DEBIAN

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to block any potential future use of the token by an unauthorized party.			
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. On ChangesList special pages such as Special:RecentChanges and Special:Watchlist, some of the rcfilters-filter-* label messages are output in HTML unescaped, leading to XSS.	2021-04-06	4.3	CVE-2021-30157 MISC DEBIAN
mediawiki -- mediawiki	An issue was discovered in MediaWiki before 1.31.12 and 1.32.x through 1.35.x before 1.35.2. On Special:NewFiles, all the mediastatistics-header-* messages are output in HTML unescaped, leading to XSS.	2021-04-06	4.3	CVE-2021-30154 MISC DEBIAN
ninjaforms -- ninja_forms	In the Ninja Forms Contact Form WordPress plugin before 3.4.34.1, low-level users, such as subscribers, were able to trigger the action, wp_ajax_nf_oauth, and retrieve the	2021-04-05	4	CVE-2021-24164 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	connection url needed to establish a connection. They could also retrieve the client_id for an already established OAuth connection.			RM MISC
ninjaforms -- ninja_forms	The AJAX action, wp_ajax_ninja_forms_sendwp_remote_install_handler, did not have a capability check on it, nor did it have any nonce protection, therefore making it possible for low-level users, such as subscribers, to install and activate the SendWP Ninja Forms Contact Form â€“ The Drag and Drop Form Builder for WordPress WordPress plugin before 3.4.34 and retrieve the client_secret key needed to establish the SendWP connection while also installing the SendWP plugin.	2021-04-05	6.5	CVE-2021-24163 CONFIRM MISC
ninjaforms -- ninja_forms	The wp_ajax_nf_oauth_disconnect from the Ninja Forms Contact Form – The Drag and Drop Form Builder for WordPress WordPress plugin before 3.4.34 had no nonce protection making	2021-04-05	5.8	CVE-2021-24166 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	it possible for attackers to craft a request to disconnect a site's OAuth connection.			
ninjaforms -- ninja_forms	In the Ninja Forms Contact Form WordPress plugin before 3.4.34, the wp_ajax_nf_oauth_connect AJAX action was vulnerable to open redirect due to the use of a user supplied redirect parameter and no protection in place.	2021-04-05	5.8	CVE-2021-24165 CONFIRM MISC
ocproducts -- composr	Composr 10.0.36 allows XSS in an XML script.	2021-04-06	4.3	CVE-2021-30150 MISC MISC
openiam -- openiam	OpenIAM before 4.2.0.3 allows Directory Traversal in the Batch task.	2021-04-06	5	CVE-2020-13419 MISC
openiam -- openiam	OpenIAM before 4.2.0.3 allows XSS in the Add New User feature.	2021-04-06	4.3	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				13418 MISC
openiam -- openiam	OpenIAM before 4.2.0.3 does not verify if a user has permissions to perform /webconsole/rest/api/* administrative actions.	2021-04-06	5.5	CVE-2020-13422 MISC
piwigo -- piwigo	SQL injection exists in Piwigo before 11.4.0 via the language parameter to admin.php?page=languages.	2021-04-02	6.5	CVE-2021-27973 MISC
pomerium -- pomerium	Pomerium from version 0.10.0-0.13.3 has an Open Redirect in the user sign-in/out process	2021-04-02	5.8	CVE-2021-29652 CONFIRM
pomerium -- pomerium	Pomerium before 0.13.4 has an Open Redirect (issue 1 of 2).	2021-04-02	5.8	CVE-2021-29651

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
redmine -- redmine	Redmine before 4.0.7 and 4.1.x before 4.1.1 allows attackers to discover the subject of a non-visible issue by performing a CSV export and reading time entries.	2021-04-06	5	CVE-2020-36308 MISC
redmine -- redmine	Redmine before 3.4.13 and 4.x before 4.0.6 mishandles markup data during Textile formatting.	2021-04-06	5	CVE-2019-25026 MISC
redmine -- redmine	Redmine before 4.0.8 and 4.1.x before 4.1.2 allows attackers to discover the names of private projects if issue-journal details exist that have changes to project_id values.	2021-04-06	5	CVE-2021-30163 MISC
redmine -- redmine	Redmine before 4.0.7 and 4.1.x before 4.1.1 has stored XSS via textile inline links.	2021-04-06	4.3	CVE-2020-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				36307 MISC
redmine -- redmine	Redmine before 4.0.7 and 4.1.x before 4.1.1 has XSS via the back_url field.	2021-04-06	4.3	CVE-2020-36306 MISC
rstudio -- shiny_server	Directory traversal in RStudio Shiny Server before 1.5.16 allows attackers to read the application source code, involving an encoded slash.	2021-04-02	5	CVE-2021-3374 MISC MISC
sannce -- smart_hd_wifi_security_camera_ean_2_950004_595317_firmware	An issue was discovered on Sannce Smart HD Wifi Security Camera EAN 2 950004 595317 devices. By default, a mobile application is used to stream over UDP. However, the device offers many more services that also enable streaming. Although the service used by the mobile application requires a password, the other streaming services do not. By initiating communication on	2021-04-02	5	CVE-2019-20464 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	the RTSP port, an attacker can obtain access to the video feed without authenticating.			
sannce -- smart_hd_wifi_security_camera_ean_2_950004_595317_firmware	An issue was discovered on Sannce Smart HD Wifi Security Camera EAN 2 950004 595317 devices. It is possible (using TELNET without a password) to control the camera's pan/zoom/tilt functionality.	2021-04-02	5	CVE-2019-20465 MISC
serenityos -- serenity	SerenityOS fixed as of c9f25bca048443e317f1994ba9b106f2386688c3 contains a buffer overflow vulnerability in LibTextCode through opening a crafted file.	2021-04-06	6.8	CVE-2021-28874 MISC MISC MISC
serenityos -- serenity	SerenityOS Unspecified is affected by: Buffer Overflow. The impact is: obtain sensitive information (context-dependent). The component is: /Userland/Libraries/LibCrypto/ASN1/DER.h Crypto::der_decode_sequence()	2021-04-06	5	CVE-2021-27343 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	function. The attack vector is: Parsing RSA Key ASN.1.			
softing -- opc_toolbox	A Cross-Site Request Forgery (CSRF) vulnerability in en/cfg_setpwd.html in Softing AG OPC Toolbox through 4.10.1.13035 allows attackers to reset the administrative password by inducing the Administrator user to browse a URL controlled by an attacker.	2021-04-02	6.8	CVE-2021-29660 MISC
svelte -- svelte	The unofficial Svelte extension before 104.8.0 for Visual Studio Code allows attackers to execute arbitrary code via a crafted workspace configuration.	2021-04-05	6.8	CVE-2021-29261 MISC MISC MISC MISC MISC
sygnoos -- popup_builder	The "All Subscribers" setting page of Popup Builder was vulnerable to reflected Cross-Site Scripting.	2021-04-05	4.3	CVE-2021-24152

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
themeum -- tutor_lms	The tutor_mark_answer_as_correct AJAX action from the Tutor LMS â€“ eLearning and online course solution WordPress plugin before 1.7.7 was vulnerable to blind and time based SQL injections that could be exploited by students.	2021-04-05	4	CVE-2021-24181 CONFIRM MISC
themeum -- tutor_lms	The tutor_quiz_builder_get_answers_by_question AJAX action from the Tutor LMS – eLearning and online course solution WordPress plugin before 1.8.3 was vulnerable to UNION based SQL injection that could be exploited by students.	2021-04-05	4	CVE-2021-24182 CONFIRM MISC
themeum -- tutor_lms	The tutor_quiz_builder_get_question_form AJAX action from the Tutor LMS – eLearning and online course solution	2021-04-05	4	CVE-2021-24183 CONFI

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	WordPress plugin before 1.8.3 was vulnerable to UNION based SQL injection that could be exploited by students.			RM MISC
themeum -- tutor_lms	The tutor_place_rating AJAX action from the Tutor LMS – eLearning and online course solution WordPress plugin before 1.7.7 was vulnerable to blind and time based SQL injections that could be exploited by students.	2021-04-05	4	CVE-2021-24185 CONFIRM MISC
themeum -- tutor_lms	The tutor_answering_quiz_question/get_answer_by_id function pair from the Tutor LMS – eLearning and online course solution WordPress plugin before 1.8.3 was vulnerable to UNION based SQL injection that could be exploited by students.	2021-04-05	4	CVE-2021-24186 CONFIRM MISC
themeum -- tutor_lms	Several AJAX endpoints in the Tutor LMS – eLearning and online course solution WordPress plugin before 1.7.7	2021-04-05	6.5	CVE-2021-24184

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	were unprotected, allowing students to modify course information and elevate their privileges among many other actions.			CONFIRM MISC
unionpayintl -- union_pay	Union Pay up to 1.2.0, for web based versions contains a CWE-347: Improper Verification of Cryptographic Signature vulnerability, allows attackers to shop for free in merchants' websites and mobile apps, via a crafted authentication code (MAC) which is generated based on a secret key which is NULL.	2021-04-06	5	CVE-2020-23533 MISC MISC MISC
unionpayintl -- union_pay	Union Pay up to 3.4.93.4.9, for android, contains a CWE-347: Improper Verification of Cryptographic Signature vulnerability, allows attackers to shop for free in merchants' websites and mobile apps, via a crafted authentication code (MAC) which is generated based on a secret key which is NULL.	2021-04-06	5	CVE-2020-36284 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
unionpayintl -- union_pay	Union Pay up to 3.3.12, for iOS mobile apps, contains a CWE-347: Improper Verification of Cryptographic Signature vulnerability, allows attackers to shop for free in merchants' websites and mobile apps, via a crafted authentication code (MAC) which is generated based on a secret key which is NULL.	2021-04-06	5	CVE-2020-36285 MISC MISC MISC
vim_project -- vim	VSCodeVim before 1.19.0 allows attackers to execute arbitrary code via a crafted workspace configuration.	2021-04-05	6.8	CVE-2021-28832 MISC MISC MISC
vm_backups_project -- vm_backups	The VM Backups WordPress plugin through 1.0 does not have CSRF checks, allowing attackers to make a logged in user unwanted actions, such as update the plugin's options, leading to a Stored Cross-Site Scripting issue.	2021-04-05	4.3	CVE-2021-24173 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
vm_backups_project -- vm_backups	The VM Backups WordPress plugin through 1.0 does not have CSRF checks, allowing attackers to make a logged in user unwanted actions, such as generate backups of the DB, plugins, and current .	2021-04-05	4.3	CVE-2021-24172 CONFIRM
w1.fi -- hostapd	In wpa_supplicant and hostapd 2.9, forging attacks may occur because AlgorithmIdentifier parameters are mishandled in tls/pkcs1.c and tls/x509v3.c.	2021-04-02	5	CVE-2021-30004 MISC
web-stat -- web-stat	When visiting a site running Web-Stat < 1.4.0, the "wts_web_stat_load_init" function used the visitorâ€™s browser to send an XMLHttpRequest request to https://wts2.one/ajax.htm?action=lookup_WP_account.	2021-04-05	5	CVE-2021-24167 CONFIRM
wire -- wire-webapp	wire-webapp is an open-source front end for Wire, a secure collaboration platform. In wire-webapp before version 2021-03-15-production.0, when being	2021-04-02	4.3	CVE-2021-21400 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	prompted to enter the app-lock passphrase, the typed passphrase will be sent into the most recently used chat when the user does not actively give focus to the input field. Input element focus is enforced programatically in version 2021-03-15-production.0.			MISC MISC CONFIRM
wso2 -- api_manager	WSO2 Management Console through 5.10 allows XSS via the carbon/admin/login.jsp msgId parameter.	2021-04-05	4.3	CVE-2020-17453 MISC MISC MISC
wuzhicms -- wuzhicms	Directory traversal in coreframe/app/template/admin/index.php in WUZHI CMS 4.1.0 allows attackers to list files in arbitrary directories via the dir parameter.	2021-04-02	4	CVE-2020-21590 MISC MISC
yomi-search_project -- yomi-search	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote	2021-04-07	4.3	CVE-2021-

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	attackers to inject an arbitrary script via unspecified vectors.			20691 MISC
yomi-search_project -- yomi-search	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-04-07	4.3	CVE-2021-20690 MISC
yomi-search_project -- yomi-search	Cross-site scripting vulnerability in Yomi-Search Ver4.22 allows remote attackers to inject an arbitrary script via unspecified vectors.	2021-04-07	4.3	CVE-2021-20689 MISC

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- ipados	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur	2021-04-02	2.1	CVE-2021-1769

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	11.2, Security Update 2021-001 Catalina, Security Update 2021-001 Mojave, watchOS 7.3, tvOS 14.4, iOS 14.4 and iPadOS 14.4. A malicious attacker with arbitrary read and write capability may be able to bypass Pointer Authentication.			MISC MISC MISC MISC
apple -- ipados	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in iOS 14.4 and iPadOS 14.4. An attacker with physical access to a device may be able to see private contact information.	2021-04-02	2.1	CVE-2021-1756 MISC
apple -- ipados	"Clear History and Website Data" did not clear the history. The issue was addressed with improved data deletion. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave, iOS 14.3 and iPadOS 14.3, tvOS 14.3. A user may be unable to fully delete browsing history.	2021-04-02	2.1	CVE-2020-29623 FEDORA FEDORA MISC MISC MISC
apple -- ipados	This issue was addressed with improved setting propagation. This issue is fixed in macOS Big Sur 11.0.1, tvOS 14.0, macOS Big Sur 11.1, Security	2021-04-02	2.7	CVE-2020-9978 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	Update 2020-001 Catalina, Security Update 2020-007 Mojave, watchOS 7.0, iOS 14.0 and iPadOS 14.0. An attacker in a privileged network position may be able to unexpectedly alter application state.			MISC MISC MISC MISC
apple -- mac_os_x	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.1, Security Update 2020-001 Catalina, Security Update 2020-007 Mojave. A malicious application may be able to bypass Privacy preferences.	2021-04-02	2.1	CVE-2020-29621 MISC
apple -- macos	A lock screen issue allowed access to contacts on a locked device. This issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.0.1. A person with physical access to an iOS device may be able to access contacts from the lock screen.	2021-04-02	2.1	CVE-2021-1755 MISC
clogica -- seo_redirection	The setting page of the SEO Redirection Plugin â€“ 301 Redirect Manager WordPress plugin through 6.3 is vulnerable to reflected Cross-Site Scripting (XSS) as user input is not properly sanitised before being output in an attribute.	2021-04-05	3.5	CVE-2021-24187 CONFIRM

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
cm-wp -- social_slider_widget	The Social Slider Widget WordPress plugin before 1.8.5 allowed Authenticated Reflected XSS in the plugin settings page as the â€˜token_errorâ€™ parameter can be controlled by users and it is directly echoed without being sanitized	2021-04-05	3.5	CVE-2021-24196 MISC CONFIRM
coreftp -- core_ftp	Buffer overflow in Core FTP LE v2.2 allows local attackers to cause a denial or service (crash) via a long string in the Setup->Users->Username editbox.	2021-04-02	2.1	CVE-2020-21588 MISC MISC
easy_contact_form_pro_project -- easy_contact_form_pro	The Easy Contact Form Pro WordPress plugin before 1.1.1.9 did not properly sanitise the text fields (such as Email Subject, Email Recipient, etc) when creating or editing a form, leading to an authenticated (author+) stored cross-site scripting issue. This could allow medium privilege accounts (such as author and editor) to perform XSS attacks against high privilege ones like administrator.	2021-04-05	3.5	CVE-2021-24168 CONFIRM
elementor -- website_builder	In the Elementor Website Builder WordPress plugin before 3.1.4, the heading widget (includes/widgets/heading.php) accepts a	2021-04-05	3.5	CVE-2021-24202

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	‘header_size’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request with this parameter set to ‘script’ and combined with a ‘title’ parameter containing JavaScript, which will then be executed when the saved page is viewed or previewed.			CONFIRM MISC
elementor -- website_builder	In the Elementor Website Builder WordPress plugin before 3.1.4, the accordion widget (includes/widgets/accordion.php) accepts a ‘title_html_tag’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request containing JavaScript in the ‘title_html_tag’ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.	2021-04-05	3.5	CVE-2021-24204 CONFIRM MISC
elementor -- website_builder	In the Elementor Website Builder WordPress plugin before 3.1.4, the divider widget (includes/widgets/divider.php) accepts an ‘html_tag’ parameter. Although the element control	2021-04-05	3.5	CVE-2021-24203 CONFIR

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request with this parameter set to 'script' and combined with a 'text' parameter containing JavaScript, which will then be executed when the saved page is viewed or previewed.			M MISC
elementor -- website_builder	In the Elementor Website Builder WordPress plugin before 3.1.4, the icon box widget (includes/widgets/icon-box.php) accepts a 'title_size' parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified 'save_builder' request containing JavaScript in the 'title_size' parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.	2021-04-05	3.5	CVE-2021-24205 CONFIRM MISC
elementor -- website_builder	In the Elementor Website Builder WordPress plugin before 3.1.4, the column element (includes/elements/column.php) accepts an â€˜html_tagâ€™ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above	2021-04-05	3.5	CVE-2021-24201 CONFIRM MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	permissions to send a modified â€˜save_builderâ€™ request containing JavaScript in the â€˜html_tagâ€™ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.			
elementor -- website_builder	In the Elementor Website Builder WordPress plugin before 3.1.4, the image box widget (includes/widgets/image-box.php) accepts a ‘title_size’ parameter. Although the element control lists a fixed set of possible html tags, it is possible for a user with Contributor or above permissions to send a modified ‘save_builder’ request containing JavaScript in the ‘title_size’ parameter, which is not filtered and is output without escaping. This JavaScript will then be executed when the saved page is viewed or previewed.	2021-04-05	3.5	CVE-2021-24206 CONFIRM MISC
eng -- knowage	Knowage Suite before 7.4 is vulnerable to reflected cross-site scripting (XSS). An attacker can inject arbitrary web script in /restful-services/publish via the 'EXEC_FROM' parameter that can lead to data leakage.	2021-04-05	3.5	CVE-2021-30056 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
eng -- knowage	A stored HTML injection vulnerability exists in Knowage Suite version 7.1. An attacker can inject arbitrary HTML in "/restful-services/2.0/analyticalDrivers" via the 'LABEL' and 'NAME' parameters.	2021-04-05	3.5	CVE-2021-30057 MISC
gitlab -- gitlab	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.4. It was possible to exploit a stored cross-site-scripting in merge request via a specifically crafted branch name.	2021-04-02	3.5	CVE-2021-22196 CONFIRM MISC MISC
ibm -- edge_application_manager	IBM Edge 4.2 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: 189441.	2021-04-05	3.5	CVE-2020-4792 XF CONFIRM
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	2021-04-05	3.5	CVE-2020-4997 XF

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 192914			CONFIRM
jh_404_logger_project -- jh_404_logger	The JH 404 Logger WordPress plugin through 1.1 doesn't sanitise the referer and path of 404 pages, when they are output in the dashboard, which leads to executing arbitrary JavaScript code in the WordPress dashboard.	2021-04-05	3.5	CVE-2021-24176 CONFIRM
linux -- linux_kernel	An issue was discovered in the Linux kernel before 5.11.3 when a webcam device exists. video_usercopy in drivers/media/v4l2-core/v4l2-ioctl.c has a memory leak for large arguments, aka CID-fb18802a338b.	2021-04-02	2.1	CVE-2021-30002 MISC MISC MISC
magnolia-cms -- magnolia_cms	Magnolia CMS From 6.1.3 to 6.2.3 contains a stored cross-site scripting (XSS) vulnerability in the setText parameter of /magnoliaAuthor/.magnolia/.	2021-04-02	3.5	CVE-2021-25893 MISC MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
never5 -- related_posts	Unvalidated input and lack of output encoding within the Related Posts for WordPress plugin before 2.0.4 lead to a Reflected Cross-Site Scripting (XSS) vulnerability within the 'lang' GET parameter while editing a post, triggered when users with the capability of editing posts access a malicious URL.	2021-04-05	3.5	CVE-2021-24180 CONFIRM
nokia -- g-120w-f_firmware	An issue was discovered on Nokia G-120W-F 3FE46606AGAB91 devices. There is Stored XSS in the administrative interface via urlfilter.cgi?add url_address.	2021-04-02	3.5	CVE-2021-30003 MISC
softing -- opc_toolbox	Softing AG OPC Toolbox through 4.10.1.13035 allows /en/diag_values.html Stored XSS via the ITEMLISTVALUES##ITEMID parameter, resulting in JavaScript payload injection into the trace file. This payload will then be triggered every time an authenticated user browses the page containing it.	2021-04-02	3.5	CVE-2021-29661 MISC
testimonial_rotator_project -- testimonial_rotator	Stored Cross-Site Scripting vulnerabilities in Testimonial Rotator 3.0.3 allow low privileged users (Contributor) to inject arbitrary JavaScript code or HTML without approval. This could lead to privilege escalation	2021-04-05	3.5	CVE-2021-24156 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				CONFIRM
themeisle -- orbit_fox	Orbit Fox by ThemeIsle has a feature to add a registration form to both the Elementor and Beaver Builder page builders functionality. As part of the registration form, administrators can choose which role to set as the default for users upon registration. This field is hidden from view for lower-level users, however, they can still supply the user_role parameter to update the default role for registration.	2021-04-05	3.5	CVE-2021-24158 CONFIRM MISC
themeisle -- orbit_fox	Orbit Fox by ThemeIsle has a feature to add custom scripts to the header and footer of a page or post. There were no checks to verify that a user had the unfiltered_html capability prior to saving the script tags, thus allowing lower-level users to inject scripts that could potentially be malicious.	2021-04-05	3.5	CVE-2021-24157 CONFIRM MISC
webdesi9 -- file_manager	In the default configuration of the File Manager WordPress plugin before 7.1, a Reflected XSS can occur on the endpoint /wp-admin/admin.php?page=wp_file_manager_properties when a payload is submitted on the User-Agent	2021-04-05	3.5	CVE-2021-24177 MISC MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	parameter. The payload is then reflected back on the web application response.			CONFIRM
wizconnected -- a60_colors_firmware	An issue was discovered in WiZ Colors A60 1.14.0. The device sends unnecessary information to the cloud controller server. Although this information is sent encrypted and has low risk in isolation, it decreases the privacy of the end user. The information sent includes the local IP address being used and the SSID of the Wi-Fi network the device is connected to. (Various resources such as wigle.net can be use for mapping of SSIDs to physical locations.)	2021-04-02	3.3	CVE-2020-11922 MISC
wizconnected -- colors_a60_firmware	An issue was discovered in WiZ Colors A60 1.14.0. Wi-Fi credentials are stored in cleartext in flash memory, which presents an information-disclosure risk for a discarded or resold device.	2021-04-02	2.1	CVE-2020-11924 MISC
wizconnected -- wiz	An issue was discovered in WiZ Colors A60 1.14.0. API credentials are locally logged.	2021-04-02	2.1	CVE-2020-11923 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
yoast -- yoast_seo	A Stored Cross-Site Scripting vulnerability was discovered in the Yoast SEO WordPress plugin before 3.4.1, which had built-in blacklist filters which were blacklisting Parenthesis as well as several functions such as alert but bypasses were found.	2021-04-05	3.5	CVE-2021-24153 MISC MISC CONFIRM