

Security fixes

You can view the open issues, resolved issues, and security fixes using the Cisco Bug Search Tool.

- Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260205) and B-Series M6 6.0(2.260205) Server Firmware Release — None, on page 2
- Security fixes in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None, on page 2
- Security fixes in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release, on page 2
- Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260143) and B-Series M6 6.0(2.260143) Server Firmware Release, on page 2
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(2.260069), C-Series M8, M7, M6 6.0(2.260069), and B-Series M6 6.0(2.260069) Server Firmware Release, on page 3
- Security fixes in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release, on page 3
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release, on page 4
- Security fixes in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None, on page 20
- Security fixes in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None, on page 20
- Security fixes in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None, on page 20
- Security fixes in Cisco UCS XE-Series M8 6.0(1.251030) Server Firmware Release — None, on page 20
- Security fixes in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None, on page 20
- Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release, on page 20
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None, on page 21
- Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release, on page 21

Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260205) and B-Series M6 6.0(2.260205) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8, M7 6.0(2.260180) and C-Series M8, M7 6.0(2.260180) Server Firmware Release — None

Security fixes in Cisco UCS B-Series M5 6.0(1.260031) Server Firmware Release

Defect ID - CSCwt77804

A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of all Cisco UCS B-series M5 servers could allow an authenticated attacker with valid credentials for a user account with the role of *user* or *admin* or an unauthenticated attacker with physical access to an affected device to bypass UEFI Secure Boot validation checks and execute unauthorized software.

This vulnerability is due to the availability of memory write commands in the UEFI Shell while UEFI Secure Boot is enabled on a device. An attacker could exploit this vulnerability by selecting the UEFI Shell boot option at boot time and using available shell commands to modify UEFI memory variables. A successful exploit could allow the attacker to manipulate the preboot environment, overwrite UEFI Secure Boot-related memory values, and execute unauthorized software on the affected device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

Cisco UCS and UCS-Based Appliances UEFI Shell Secure Boot Bypass Vulnerability

Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(2.260143) and B-Series M6 6.0(2.260143) Server Firmware Release

Defect ID - CSCwt77804

A vulnerability in the Unified Extensible Firmware Interface (UEFI) Shell implementation of all Cisco UCS B-series and C-series M6, M7, and M8 servers could allow an authenticated attacker with valid credentials for a user account with the role of *user* or *admin* or an unauthenticated attacker with physical access to an affected device to bypass UEFI Secure Boot validation checks and execute unauthorized software.

This vulnerability is due to the availability of memory write commands in the UEFI Shell while UEFI Secure Boot is enabled on a device. An attacker could exploit this vulnerability by selecting the UEFI Shell boot option at boot time and using available shell commands to modify UEFI memory variables. A successful

exploit could allow the attacker to manipulate the preboot environment, overwrite UEFI Secure Boot-related memory values, and execute unauthorized software on the affected device.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:

Cisco UCS and UCS-Based Appliances UEFI Shell Secure Boot Bypass Vulnerability

Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(2.260069), C-Series M8, M7, M6 6.0(2.260069), and B-Series M6 6.0(2.260069) Server Firmware Release

Defect ID - CSCwr69876

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-0033	Improper access control within AMD SEV-SNP could allow an admin privileged attacker to write to the RMP during SNP initialization, potentially resulting in a loss of SEV-SNP guest memory integrity.
CVE-2025-29943	Improper write condition handling within AMD CPUs could allow an admin-privileged attacker to modify the configuration of the CPU pipeline, potentially resulting in the corruption of the stack pointer inside an SEV-SNP guest.
CVE-2025-48514	Insufficient Granularity of Access Control in SEV firmware can allow a privileged attacker to create a SEV-ES Guest to attack SNP guest, potentially resulting in a loss of confidentiality.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security fixes in Cisco UCS B-Series M5 6.0(1.260012) Server Firmware Release

Defect ID - CSCwq34278

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-20064	Improper input validation in the UEFI FlashUcAcmSmm module on certain Intel reference platforms may allow a privileged local attacker to execute arbitrary code and escalate privileges, severely impacting system confidentiality, integrity, and availability.
CVE-2025-20027	Improper input validation in the UEFI WheaERST module on certain Intel reference platforms may allow a privileged local attacker to escalate privileges, potentially impacting system confidentiality, integrity, and availability.
CVE-2025-20028	A time-of-check time-of-use (TOCTOU) race condition in the UEFI WheaERST SMM module on certain Intel reference platforms may allow a privileged local attacker to escalate privileges, impacting system confidentiality, integrity, and availability.
CVE-2025-20105	Improper input validation in certain UEFI firmware SMM modules on Intel reference platforms may allow a privileged local attacker to execute arbitrary code with low complexity, resulting in a high impact on system confidentiality, integrity, and availability.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(2.260040), XE-Series M8 6.0(2.260042), C-Series M8, M7, M6 6.0(2.260044), and B-Series M6 6.0(2.260040) Server Firmware Release

Defect ID - CSCwr50426

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2024-13176	A timing side-channel vulnerability in OpenSSL's ECDSA signature computation may allow an attacker with local access or a low-latency network connection to potentially recover a private key, particularly when using the NIST P-521 curve.
CVE-2024-5535	A buffer overread flaw in OpenSSL's SSL_select_next_proto API function, triggered when called with an empty client protocols buffer, may cause an application crash or allow up to 255 bytes of private memory to be sent to a peer.
CVE-2024-9143	Use of low-level GF(2^m) elliptic curve APIs in OpenSSL with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes, potentially resulting in an application crash or remote code execution.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr81218

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-48384	A link following vulnerability in Git stems from inconsistent handling of carriage return characters in configuration files; when initializing a submodule with a trailing carriage return in its path, the altered path may lead to an incorrect checkout location, potentially allowing arbitrary code execution if a symlink points to a malicious hook script.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr83710

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2021-0920	A race condition in the Unix domain socket implementation (unix_scm_to_skb inaf_unix.c) of the Linux kernel may lead to a use-after-free vulnerability, allowing a local attacker to potentially escalate privileges or cause a system crash.
CVE-2024-53150	An out-of-bounds read vulnerability in the Linux kernel's ALSA USB-audio driver, caused by insufficient validation of descriptor lengths (bLength), may allow an attacker with physical access to use a malicious USB device to disclose sensitive kernel memory or cause a denial of service.
CVE-2025-38352	A race condition in the Linux kernel's POSIX CPU timer handling between the handle_posix_cpu_timers() and posix_cpu_timer_del() functions may result in a use-after-free scenario, potentially allowing a local user to escalate privileges or crash the system.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws61975

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2015-5477	An error in the handling of TKEY queries in ISC BIND 9 can be exploited by a remote attacker to trigger a REQUIRE assertion failure, causing the named daemon to exit and resulting in a denial of service.

CVE ID	Description
CVE-2016-2776	A flaw in the way ISC BIND 9 constructs responses to specific queries can lead to an assertion failure in buffer.c, allowing a remote attacker to cause the named process to crash and exit unexpectedly.
CVE-2023-50387	Known as **KeyTrap**, this vulnerability in DNSSEC-validating resolvers (such as BIND and Unbound) allows a remote attacker to cause extreme CPU exhaustion and a denial of service by providing a specially crafted DNSSEC-signed zone with complex resource record combinations.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws65661

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2010-2252	Wget 1.12 and earlier allows remote attackers to write to arbitrary files via a 302 redirect to a URL with a different filename when the -O (output document) option is used, as Wget uses the filename from the redirected URL rather than the original.
CVE-2014-4877	Wget before 1.16 allows remote FTP servers to write to arbitrary files, and potentially execute code, via a symlink attack in a directory listing during a recursive retrieval.
CVE-2016-4971	Wget before 1.18 allows remote servers to write to arbitrary files by redirecting an HTTP request to an FTP URL, which causes Wget to save the file with a name provided by the FTP server rather than the original HTTP filename.
CVE-2017-6508	Wget before 1.19.1 allows remote attackers to inject arbitrary HTTP headers (CRLFinjection) via a crafted URL, which could lead to session hijacking or other header-based attacks.
CVE-2018-0494	Wget before 1.19.5 allows remote attackers to bypass intended cookie access restrictions via a malformed Set-Cookie header, potentially leading to cookie injection or overwriting.
CVE-2021-31879	Wget before 1.21.1 does not properly handle certain HTTP response headers, such as Content-Length, which may allow a remote attacker to bypass security controls or cause unexpected behavior.
CVE-2024-10524	A path traversal vulnerability exists in certain versions of WPS Office for Windows that allows an attacker to achieve arbitrary code execution via a specially crafted file.
CVE-2024-38428	Wget before 1.24.5 is vulnerable to a flaw where it fails to properly parse user info in a URI, which could be exploited to bypass security filters or lead to credential disclosure in certain configurations.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws68419

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2009-5155	An off-by-one error in the strfmon_l function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large precision value.
CVE-2010-0015	The NIS+ implementation in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted NIS+ directory name that triggers a buffer overflow.
CVE-2011-5320	The tar implementation in BusyBox before 1.20.0 allows remote attackers to create or overwrite arbitrary files via a directory traversal attack in a tar header.
CVE-2012-4412	An integer overflow in the strcoll function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string.
CVE-2012-4424	A stack-based buffer overflow in the strcoll function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string.
CVE-2013-4237	The read dir_r function in the GNU C Library (glibc) does not properly handle certain directory entries, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash).
CVE-2013-4458	A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large number of AF_INET6 addresses.
CVE-2013-4788	The PTR_MANGLE implementation in the GNU C Library (glibc) does not properly initialize the guard value, which allows local attackers to bypass the pointer-guarding protection mechanism.
CVE-2014-4043	The posix_spawn_file_actions_addopen function in the GNU C Library (glibc) before 2.20 does not copy its path argument, which allows context-dependent attackers to trigger a use-after-free vulnerability.
CVE-2014-6040	An out-of-bounds read in the iconv function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted multibyte sequence.
CVE-2014-7817	The wordexp function in the GNU C Library (glibc) allows context-dependent attackers to execute arbitrary commands via a crafted string that triggers command substitution even when WRDE_NOCMD is specified.

CVE ID	Description
CVE-2014-8121	The nss_files implementation in the GNU C Library (glibc) does not properly handle certain database files, which allows local attackers to cause a denial of service (infinite loop) or corrupt the database.
CVE-2014-9402	The getnetbyname function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (infinite loop) via a crafted DNS response.
CVE-2014-9761	A stack-based buffer overflow in the nan function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a long string.
CVE-2015-1781	A buffer overflow in the gethostbyname_r function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long host name.
CVE-2015-5180	A NULL pointer dereference in the res_query function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2015-8776	An out-of-bounds access in the strftime function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted format string.
CVE-2015-8777	The LD_POINTER_GUARD environment variable in the GNU C Library (glibc) allows local attackers to bypass the pointer-guarding protection mechanism by disabling it.
CVE-2015-8778	An integer overflow in the hcreate function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large number of elements.
CVE-2015-8779	A stack-based buffer overflow in the catopen function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long catalog name.
CVE-2015-8982	A buffer overflow in the strftime function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted format string.
CVE-2015-8983	An integer overflow in the _IO_wstr_overflow function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large string.
CVE-2015-8984	An out-of-bounds read in the fnmatch function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a crafted pattern.
CVE-2015-8985	The pop_fail_stack function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (assertion failure and crash) via vectors related to extended regular expression processing.

CVE ID	Description
CVE-2016-10228	An out-of-bounds write in the iconv function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted multibyte sequence.
CVE-2016-10739	A buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large number of AF_INET6 addresses.
CVE-2016-1234	A stack-based buffer overflow in the glob function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long path.
CVE-2016-3075	A stack-based buffer overflow in the getnetbyname function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2016-3706	A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion, due to an incomplete fix for CVE-2013-4458.
CVE-2016-4429	A stack-based buffer overflow in the clntudp_call function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC response.
CVE-2017-12132	The DNS stub resolver in the GNU C Library (glibc) before 2.26 will solicit largeUDP responses when EDNS support is enabled, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
CVE-2017-15670	An off-by-one error in the glob function in the GNU C Library (glibc) before 2.27leads to a heap-based buffer overflow when processing home directories using the ~ operator followed by a long string.
CVE-2017-15671	The glob function in the GNU C Library (glibc) before 2.27 could skip freeing allocated memory when processing the ~ operator with a long username, potentially leading to a denial of service (memory leak).
CVE-2017-16997	The elf/dl-load.c implementation in the GNU C Library (glibc) does not properly handle certain checks, which allows local attackers to bypass security restrictions via a crafted shared object.
CVE-2017-8804	The memmove and memcpy implementations in the GNU C Library (glibc) for x86_64 do not properly handle overlapping memory regions in certain cases, which allows context-dependent attackers to cause a denial of service (crash) or possibly have other unspecified impact.
CVE-2018-1000001	A buffer underflow in the realpath function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted path.
CVE-2018-11236	An integer overflow in the __vfprintf_internal function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large precision value.

CVE ID	Description
CVE-2018-6485	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (glibc) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
CVE-2019-1010023	A buffer overflow in the ld.so dynamic loader in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted environment variable.
CVE-2019-19126	The GNU C Library (glibc) before 2.31 does not properly handle the LD_PRELOAD environment variable for SUID binaries, which allows local attackers to bypass security restrictions.
CVE-2019-25013	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the EUC-KR character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2019-9169	A heap-based buffer overflow in the regexec function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted regular expression.
CVE-2020-10029	A stack-based buffer overflow in the cosl function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a large input value.
CVE-2020-1751	A stack-based buffer overflow in the _dl_open function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted shared object path.
CVE-2020-1752	A use-after-free vulnerability in the glob function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted path.
CVE-2020-27618	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the IBM1364 character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2020-29573	A buffer overflow in the printf function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a large precision value.
CVE-2021-27645	A double-free vulnerability in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2021-3326	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the ISO-2022-JP-3 character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2021-33574	A use-after-free vulnerability in the mq_notify function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.

CVE ID	Description
CVE-2021-35942	A buffer overflow in the wordexp function in the GNU C Library (glibc) allows context-dependent attackers to cause a denial of service (crash) via a long string.
CVE-2021-3999	A buffer overflow in the getcwd function in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long path.
CVE-2022-23218	A stack-based buffer overflow in the svcunix_create function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC request.
CVE-2022-23219	A stack-based buffer overflow in the clnt_create function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted RPC request.
CVE-2023-4527	A stack-based buffer overflow in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a large DNS response received over TCP.
CVE-2023-4806	A use-after-free vulnerability in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2023-4813	A use-after-free vulnerability in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (crash) via a crafted DNS response.
CVE-2023-4911	A buffer overflow in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable allows a local attacker to execute arbitrary code with elevated privileges.
CVE-2023-5156	A memory leak in the getaddrinfo function in the GNU C Library (glibc) allows remote attackers to cause a denial of service (memory exhaustion) via a crafted DNS response.
CVE-2024-2961	A buffer overflow in the iconv function in the GNU C Library (glibc) when converting to the ISO-2022-CN-EXT character set allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2024-33599	A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2024-33600	A NULL pointer dereference in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) via a crafted request.
CVE-2024-33601	A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.

CVE ID	Description
CVE-2024-33602	CVE-2024-33602A buffer overflow in the nscd (name service cache daemon) in the GNU C Library (glibc) allows local attackers to cause a denial of service (crash) or possibly execute arbitrary code.
CVE-2025-0395	A buffer overflow in the assert() function in the GNU C Library (glibc) versions 2.13 to 2.40 occurs because insufficient space is allocated for the failure message, potentially leading to a denial of service.
CVE-2025-4802	A vulnerability in the GNU C Library (glibc) versions 2.27 to 2.38 allows a local attacker to load malicious shared libraries and escalate privileges via an untrusted LD_LIBRARY_PATH in statically compiled setuid binaries that call dlopen.
CVE-2025-5702	A vulnerability in the optimized strcmp implementation for Power10 processors in the GNU C Library (glibc) version 2.39 and later improperly initializes vector registers, potentially leading to data corruption or altered control flow.
CVE-2025-8058	A double-free vulnerability in the regcomp function in the GNU C Library (glibc) versions 2.4 to 2.41 occurs during bracket expression parsing when a memory allocation failure takes place, potentially allowing arbitrary code execution.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws68836

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2007-5116	A buffer overflow in the polymorphic opcode support in the Regular Expression Engine (regcomp.c) in Perl 5.8 allows context-dependent attackers to execute arbitrary code by switching from byte to Unicode (UTF) characters in a regular expression.
CVE-2008-1927	A double free vulnerability in Perl 5.8.8 allows context-dependent attackers to cause a denial of service (memory corruption and crash) via a crafted regular expression containing UTF-8characters.
CVE-2008-5302	A race condition in the rmtree function in File::Path in Perl 5.8.8 and 5.10.0 allows local users to create arbitrary setuid binaries via a symlink attack.
CVE-2008-5303	A race condition in the rmtree function in File::Path in Perl 5.8.8 allows local users to delete arbitrary files via a symlink attack, representing a regression of a previous security fix.
CVE-2010-1168	The Safe (aka Safe.pm) module before 2.25 for Perl allows context-dependent attackers to bypass intended access restrictions and execute arbitrary code via vectors involving implicitly called methods such as DESTROY and AUTOLOAD.

CVE ID	Description
CVE-2010-1447	The Safe (aka Safe.pm) module 2.26 and earlier for Perl allows context-dependent attackers to bypass access restrictions and execute arbitrary code via vectors involving subroutine references and delayed execution.
CVE-2010-2761	The multipart_init function in CGI.pm before 3.50 uses a hardcoded MIME boundary string, which allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks.
CVE-2010-4410	A CRLF injection vulnerability in the header function in CGI.pm before 3.50 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via newline characters.
CVE-2011-0761	Perl 5.10.x allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) by injecting arguments into functions such as getpeername, readdir, and closedir.
CVE-2011-1487	The lc, lcfirst, uc, and ucfirst functions in Perl 5.10.x through 5.13.x do not apply the taint attribute to return values, allowing attackers to bypass taint protection mechanisms via crafted strings.
CVE-2011-2939	An off-by-one error in the decode_xs function in the Encode module for Perl allows context-dependent attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted Unicode string.
CVE-2011-3597	An eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to execute arbitrary commands via the new constructor.
CVE-2011-4116	The _is_safe function in the File::Temp module for Perl does not properly handle symlinks, which could allow a local attacker to bypass security checks.
CVE-2012-5195	A heap-based buffer overflow in the Perl_repeatcpy function in Perl allows context-dependent attackers to cause a denial of service or execute arbitrary code via the 'x' string repeat operator.
CVE-2012-5526	CGI.pm before 3.63 for Perl does not properly escape newlines in Set-Cookie or P3P headers, allowing remote attackers to inject arbitrary headers into HTTP responses.
CVE-2012-6329	The Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and method names, allowing context-dependent attackers to execute arbitrary commands via crafted translation strings.
CVE-2013-1667	The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.
CVE-2013-7422	An integer underflow in the regular expression engine (regcomp.c) in Perl before 5.20 allows context-dependent attackers to execute arbitrary code or cause a denial of service via long digit strings.

CVE ID	Description
CVE-2014-4330	The Dumper method in Data::Dumper before 2.154 allows context-dependent attackers to cause a denial of service (stack exhaustion and crash) via deeply nested Array-References.
CVE-2015-8853	The regular expression engine in Perl before 5.24.0 allows context-dependent attackers to cause a denial of service (infinite loop and high CPU usage) via crafted UTF-8 data.
CVE-2016-1238	Perl 5.x before 5.22.3 and 5.24.1 does not properly remove the current directory (".") from the module include path (@INC), allowing local users to gain privileges via a Trojan horse module.
CVE-2016-2381	Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in the envp array.
CVE-2016-6185	The XSLoader::load method in Perl does not properly locate shared object (.so) files when called in a string eval, potentially allowing local users to execute arbitrary code via a malicious library.
CVE-2018-12015	The Archive::Tar module in Perl through 5.26.2 allows remote attackers to bypass directory-traversal protection and overwrite arbitrary files via an archive containing a symlink and a regular file with the same name.
CVE-2018-18311	Perl before 5.26.3 and 5.28.1 has a buffer overflow vulnerability via a crafted regular expression that triggers invalid write operations.
CVE-2018-6913	A heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
CVE-2020-10543	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of specific instructions in the regular expression engine, potentially leading to instruction injection.
CVE-2020-12723	A buffer overflow vulnerability in the regular expression compiler (regcomp.c) in Perl before 5.30.3 occurs during recursive calls to S_study_chunk.
CVE-2020-16156	CPAN 2.28 allows a signature verification bypass, which could allow an attacker to bypass security checks for Perl modules downloaded from the network.
CVE-2023-31484	CPAN.pm before 2.35 and Perl before 5.38.0 do not verify TLS certificates when downloading distributions over HTTPS, exposing users to man-in-the-middle attacks.
CVE-2023-47038	A heap-based buffer overflow vulnerability was found in Perl 5.30.0 through 5.38.0 when compiling a crafted regular expression with illegal Unicode properties.

CVE ID	Description
CVE-2024-56406	A heap buffer overflow vulnerability in Perl's tr operator occurs when processing non-ASCII bytes, potentially leading to a denial of service or arbitrary code execution.
CVE-2025-40909	A race condition in Perl threads during directory handle cloning can cause the current working directory to change unexpectedly, potentially allowing a local attacker to trick threads into loading malicious code.The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr84274

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2025-27363	An out-of-bounds write vulnerability in FreeType versions 2.13.0 and below occurs when parsing font subglyph structures in TrueType GX and variable font files; improper data type assignment leads to a buffer wraparound and undersized heap allocation, potentially allowing arbitrary code execution.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwr84317

This product includes third-party Software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2023-38545	A high-severity heap-based buffer overflow vulnerability in curl's SOCKS5 proxy handshake occurs when a host name longer than 255 bytes is incorrectly copied into a target buffer during a slow handshake, potentially allowing a malicious proxy to execute arbitrary code on the client.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwq11344

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-1999-0289	The Apache web server for Win32 may provide access to restricted files when a dot(.) is appended to a requested URL, potentially allowing unauthorized file disclosure.

CVE ID	Description
CVE-1999-0678	A default configuration of Apache on Debian GNU/Linux sets the ServerRoot to/usr/doc, which allows remote users to read documentation files for the entire server.
CVE-2010-1151	A race condition in the mod_auth_shadow module for the Apache HTTP Server allows remote attackers to bypass authentication and read or modify data via improper interaction with an external helper application.
CVE-2023-31122	An out-of-bounds read vulnerability in the mod_macro module of Apache HTTP Server versions through 2.4.57 allows an attacker to cause a crash or obtain sensitive information when processing long macros.
CVE-2023-38709	Faulty input validation in the core of Apache HTTP Server through version 2.4.58 allows malicious or exploitable backend content generators to split HTTP responses, potentially leading to cache poisoning or XSS.
CVE-2023-43622	A flaw in the mod_http2 module allows an attacker opening an HTTP/2 connection with an initial window size of 0 to block handling of that connection indefinitely, exhausting worker resources in a "slow loris" style attack.
CVE-2023-45802	When an HTTP/2 stream is reset by a client, memory resources may not be reclaimed immediately, allowing a client to grow the server's memory footprint and potentially cause a denial of service.
CVE-2024-24795	An HTTP response splitting vulnerability in multiple Apache HTTP Server modules allows an attacker to inject malicious response headers into backend applications, leading to HTTP desynchronization attacks.
CVE-2024-27316	The Apache HTTP Server fails to limit the amount of HTTP/2 CONTINUATION frames sent within a single stream, which can lead to memory exhaustion and a denial of service condition.
CVE-2024-36387	Serving WebSocket protocol upgrades over an HTTP/2 connection in Apache HTTP Server could result in a null pointer dereference, leading to a crash of the server process.
CVE-2024-38472	A Server-Side Request Forgery (SSRF) vulnerability in Apache HTTP Server on Windows allows an attacker to potentially leak NTLM hashes to a malicious server via crafted requests or content.
CVE-2024-38473	An encoding problem in the mod_proxy module allows request URLs with incorrect encoding to be sent to backend services, potentially bypassing authentication via crafted requests.
CVE-2024-38474	A substitution encoding issue in mod_rewrite allows an attacker to execute scripts in directories permitted by configuration but not directly reachable by URL, or disclose script source code meant only for CGI execution.
CVE-2024-38475	Improper escaping of output in mod_rewrite allows an attacker to map URLs to filesystem locations that are permitted to be served but are not intended to be directly reachable, potentially resulting in code execution.

CVE ID	Description
CVE-2024-38476	Vulnerabilities in the core of Apache HTTP Server allow information disclosure, SSRF, or local script execution via backend applications whose response headers are malicious or exploitable.
CVE-2024-38477	A null pointer dereference in the mod_proxy module of Apache HTTP Server allows an attacker to crash the server via a specially crafted malicious request.
CVE-2024-39573	A potential SSRF vulnerability in mod_rewrite allows an attacker to cause unsafe RewriteRules to unexpectedly set up URLs to be handled by mod_proxy, bypassing intended access controls.
CVE-2024-40898	An SSRF vulnerability in Apache HTTP Server on Windows with mod_rewrite in server/vhost context allows potential leakage of NTLM hashes to a malicious server via crafted requests.
CVE-2025-3891	A flaw in the mod_auth_openidc module for Apache HTTP Server allows a remote attacker to trigger a denial of service by sending an empty POST request when the OIDCPreservePost directive is enabled.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCws68830

This product includes third-party software that is affected by the vulnerabilities identified by the following Common Vulnerabilities and Exposures (CVE) IDs:

CVE ID	Description
CVE-2005-3962	An integer overflow in the format string functionality (Perl_sv_vcatpvfn) in Perl 5.8.6 and 5.9.2 allows attackers to overwrite arbitrary memory or execute arbitrary code via format string specifiers with large values.
CVE-2005-4278	An untrusted search path vulnerability in Perl before 5.8.7-r1 on Gentoo Linux allows local users in the portage group to gain privileges via a malicious shared object in the Portage temporary build directory.
CVE-2007-5116	A buffer overflow in the polymorphic opcode support in the Regular Expression Engine (regcomp.c) in Perl 5.8 allows context-dependent attackers to execute arbitrary code by switching from byte to Unicode characters in a regular expression.
CVE-2010-1158	An integer overflow in the regular expression engine in Perl 5.8.x allows context-dependent attackers to cause a denial of service (stack consumption and crash) by matching a crafted regular expression against a long string.
CVE-2011-2728	The bsd_glob function in the File::Glob module for Perl before 5.14.2 allows context-dependent attackers to cause a denial of service (crash) via a glob expression with the GLOB_ALTDIRFUNC flag, triggering an uninitialized pointer dereference.

CVE ID	Description
CVE-2011-2939	An off-by-one error in the decode_xs function in the Encode module for Perl allows context-dependent attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted Unicode string.
CVE-2012-6329	The Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and method names, allowing context-dependent attackers to execute arbitrary commands via crafted translation strings.
CVE-2013-1667	The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.
CVE-2014-4330	The Dumper method in Data::Dumper before 2.154 allows context-dependent attackers to cause a denial of service (stack exhaustion and crash) via deeply nested Array-References.
CVE-2015-8853	The regular expression engine in Perl before 5.24.0 allows context-dependent attackers to cause a denial of service (infinite loop and high CPU usage) via crafted UTF-8 data.
CVE-2016-1238	Perl 5.x before 5.22.3 and 5.24.1 does not properly remove the current directory (".") from the module include path (@INC), allowing local users to gain privileges via a Trojan horse module.
CVE-2016-2381	Perl might allow context-dependent attackers to bypass the taint protection mechanism in a child process via duplicate environment variables in the envp array.
CVE-2017-12814	A stack-based buffer overflow in the CPerlHost::Add method in win 32/perlhost.hin Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 on Windows allows attackers to execute arbitrary code via a long environment variable.
CVE-2017-12837	A heap-based buffer overflow in the S_regatom function in regcomp.c in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service via a regular expression with a \N{} escape and the case-insensitive modifier.
CVE-2017-12883	A buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to disclose sensitive information or cause a denial of service via a crafted regular expression with an invalid \N{U+...} escape.
CVE-2018-12015	The Archive::Tar module in Perl through 5.26.2 allows remote attackers to bypass directory-traversal protection and overwrite arbitrary files via an archive containing a symlink and a regular file with the same name.
CVE-2018-18311	An integer overflow in the Perl_my_setenv function in Perl before 5.26.3 and 5.28.1 allows local attackers to cause a denial of service or execute arbitrary code via a large environment variable.

CVE ID	Description
CVE-2018-18312	A heap-based buffer overflow in the S_handle_regex_sets function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted regular expression.
CVE-2018-18313	A heap-based buffer read overflow in the S_grok_bslash_N function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to disclose sensitive information from process memory via a crafted regular expression.
CVE-2018-18314	A heap-based buffer overflow in the S_regatom function in regcomp.c in Perl before 5.26.3 and 5.28.1 allows remote attackers to cause a denial of service or execute arbitrary code via a crafted regular expression.
CVE-2018-6913	A heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
CVE-2020-10543	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of specific instructions in the regular expression engine, potentially leading to instruction injection.
CVE-2020-12723	A buffer overflow vulnerability in the regular expression compiler (regcomp.c) in Perl before 5.30.3 occurs during recursive calls to S_study_chunk.
CVE-2022-48522	A stack-based crash (infinite recursion) in the S_find_uninit_var function in Perl 5.34.0 occurs when attempting to print warning messages, potentially leading to a denial of service.
CVE-2023-31484	CPAN.pm before 2.35 and Perl before 5.38.0 do not verify TLS certificates when downloading distributions over HTTPS, exposing users to man-in-the-middle attacks.
CVE-2023-31486	HTTP::Tiny before 0.083, a Perl core module, has an insecure default TLS configuration where users must opt in to verify certificates, potentially exposing applications to man-in-the-middle attacks.
CVE-2023-47039	A binary hijacking vulnerability in Perl for Windows occurs because it relies on the system path to find the shell (cmd.exe) and initially searches the current working directory, allowing local privilege escalation.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security fixes in Cisco UCS XE-Series M8 Server Firmware Release, 6.0(1.260001) — None

Security fixes in Cisco UCS C-Series M8 6.0(1.250194) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8 6.0(1.252114), M7, M6 6.0(1.250179), B-Series M6, M5 6.0(1.250169), and C-Series M8, M7, M6 6.0(1.250192) Server Firmware Release — None

Security fixes in Cisco UCS XE-Series M8 6.0(1.251030) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8 6.0(1.252039) Server Firmware Release — None

Security fixes in Cisco UCS C-Series M8, M7, M6 6.0(1.250174) Server Firmware Release

This section provides a brief description of the security fixes.

Defect ID - CSCwq36167

The Cisco UCS C-Series M6 Rack Servers include an Intel CPU that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- **CVE-2025-20067** — Observable timing discrepancy in firmware for some Intel(R) CSME and Intel(R) SPS may allow a privileged user to potentially enable information disclosure via local access.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Defect ID - CSCwq36171

The Cisco UCS C-Series M7 Rack Servers include an Intel CPU that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) IDs:

- **CVE-2025-21096** — Improper buffer restrictions in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.
- **CVE-2025-20053** — Improper buffer restrictions for some Intel(R) Xeon(R) Processor firmware with SGX enabled may allow a privileged user to potentially enable escalation of privilege via local access.
- **CVE-2025-24305** — Insufficient control flow management in the Alias Checking Trusted Module (ACTM) firmware for some Intel(R) Xeon(R) processors may allow a privileged user to potentially enable escalation of privilege via local access.
- **CVE-2025-20613** — Predictable Seed in Pseudo-Random Number Generator (PRNG) in the firmware for some Intel(R) TDX may allow an authenticated user to potentially enable information disclosure via local access.
- **CVE-2025-21090** — Missing reference to active allocated resource for some Intel(R) Xeon(R) processors may allow an authenticated user to potentially enable denial of service via local access.
- **CVE-2025-22853** — Improper synchronization in the firmware for some Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.

Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250122), B-Series M6, M5 6.0(1.250127), and C-Series M8, M7, M6 6.0(1.250131) Server Firmware Release — None

Security fixes in Cisco UCS X-Series M8, M7, M6 6.0(1.250120), B-Series M6, M5 6.0(1.250126), and C-Series M8, M7, M6 6.0(1.250127) Server Firmware Release

This section provides a brief description of the security fixes.

Defect ID - CSCwm98102

The Cisco products UCS B-Series Blade Servers, UCS C-Series Rack Servers and UCS X-Series Compute Nodes may include an optional Trusted Platform Module (TPM) 2.0 that is affected by the vulnerability identified by the following Common Vulnerability and Exposures (CVE) ID:

- **CVE-2025-2884** — TCG TPM2.0 Reference implementation's CryptHmacSign helper function is vulnerable to Out-of-Bounds read due to the lack of validation the signature scheme with the signature key's algorithm. See Errata Revision 1.83 and advisory TCGVRT0009 for TCG standard TPM2.0.

  Cisco UCS servers equipped with one of the following optional TPM modules:

- UCSX-TPM2-002
- UCSX-TPM-002C
- UCS-TPM-002D
- UCSX-TPM-002D

The affected third-party software component has been upgraded to a version that includes fixes for the vulnerability. Future versions of the product(s) will not be affected by this vulnerability.