Sensus Approved Updates

July 7, 2025

The following updates were released by Debian and included in Unified environments in June 2025. Sensus has reviewed these updates and applied them to our Base Station environments for validation. Security updates for Unified v2.8.1 and v2.9.3 are included in this report.

Please review the below updates for installation in your environment. Sensus recommends applying any changes to a Test/Quality Assurance environment before releasing to a production environment.

For additional information and updates please visit https://www.xylem.com/en-us/about-xylem/cybersecurity/sensus-product-security/

Unified v2.8.1 Security Updates

This table describes the security updates available for Unified v2.8.1 base stations since the last update, through **2025-06-30**.

Date	Package	CVE(s)	Synopsis	Hardware Version
2025-05-26	krb5-locales	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens • Non-maintainer upload by the ELTS Security Team. • CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c • Non-maintainer upload by the ELTS	

Date	Package	CVE(s)	Synopsis	Hardware Version
			Team. • CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	
2025-05-26	libk5crypto3	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype()	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens • Non-maintainer upload by the ELTS Security Team. • CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c • Non-maintainer upload by the ELTS Team. • CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	
2025-05-26	libglib2.0-data	CVE-2025-4373 CVE-2024-52533 CVE-2024-	• Non-maintainer upload by the ELTS team. • Fix CVE-2025-4373: A flaw was	M400 M410 R100E R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
		34397 CVE-2023-29499 CVE-2023-32611 CVE-2023-32665 CVE-2021-3800 CVE-2021-28153 CVE-2021-27218 CVE-2021-27219	found in GLib, which is vulnerable to an integer overflow in the g_string_insert_unichar() function. When the position at which to insert the character is large, the position will overflow, leading to a buffer underwrite. • Add patch and define the inline keyword in gmem.h to avoid FTBFS in reverse-dependencies which require the header file. • Non-maintainer upload by the ELTS Team. • CVE-2024-52533: SOCKS4a proxy buffer overflow • Non-maintainer upload the ELTS team. • Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact. • Non-maintainer upload by the ELTS Team • Add debian/salsa-ci.yml using lts-team/pipeline for jessie • CVE-2023-29499: GVariant deserialization fails to validate that the input conforms to the expected format, leading to denial of service. • CVE-2023-32611: GVariant deserialization is vulnerable to a slowdown issue where a crafted GVariant can cause excessive processing, leading to denial of	S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			service. • CVE-2023-32665: GVariant deserialization is vulnerable to an exponential blowup issue where a crafted GVariant can cause excessive processing, leading to denial of service. • CVE-2021-3800: information leak using CHARSETALIASDIR envvar. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-28153: When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.) • Fix CVE-2021-27218: If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation. • Fix CVE-2021-27219: The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.	
2025-05-26	libgssapi-krb5-2	CVE-2025-3576 CVE-2024-26462 CVE-2024-	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability	M400 M410 R100E R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
		26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in	S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			/krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens • Non-maintainer upload by the ELTS Security Team. • CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c • Non-maintainer upload by the ELTS Team. • CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	
2025-05-26	libkrb5-3	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			• Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• CVE-2024-37371: Invalid GSS memory reads with manipulated tokens • Non-maintainer upload by the ELTS Security Team. • CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c • Non-maintainer upload by the ELTS Team. • CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	
2025-05-26	libkrb5support0	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371 CVE-2023-36054 CVE-2022-42898	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens • Non-maintainer upload by the ELTS Security Team. • CVE-2023-36054: Freeing of uninitialized pointer in kadm_rpc_xdr.c • Non-maintainer upload by the ELTS	

Date	Package	CVE(s)	Synopsis	Hardware Version
			Team. • CVE-2022-42898: Prevent integer overflows in PAC parsing; potentially critical for 32-bit KDCs or when cross-realm acts maliciously.	
2025-05-26	libglib2.0-0	CVE-2025-4373 CVE-2024-52533 CVE-2024-34397 CVE-2023-29499 CVE-2023-32611 CVE-2023-32665 CVE-2021-3800 CVE-2021-28153 CVE-2021-27218 CVE-2021-27219	• Non-maintainer upload by the ELTS team. • Fix CVE-2025-4373: A flaw was found in GLib, which is vulnerable to an integer overflow in the g_string_insert_unichar() function. When the position at which to insert the character is large, the position will overflow, leading to a buffer underwrite. • Add patch and define the inline keyword in gmem.h to avoid FTBFS in reverse-dependencies which require the header file. • Non-maintainer upload by the ELTS Team. • CVE-2024-52533: SOCKS4a proxy buffer overflow • Non-maintainer upload the ELTS team. • Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact. • Non-maintainer upload by the ELTS Team • Add debian/salsa-ci.yml using lts-	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			team/pipeline for jessie • CVE-2023-29499: GVariant deserialization fails to validate that the input conforms to the expected format, leading to denial of service. • CVE-2023-32611: GVariant deserialization is vulnerable to a slowdown issue where a crafted GVariant can cause excessive processing, leading to denial of service. • CVE-2023-32665: GVariant deserialization is vulnerable to an exponential blowup issue where a crafted GVariant can cause excessive processing, leading to denial of service. • CVE-2021-3800: information leak using CHARSETALIASDIR envvar. • Non-maintainer upload by the ELTS team. • Fix CVE-2021-28153: When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.) • Fix CVE-2021-27218: If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length	

Date	Package	CVE(s)	Synopsis	Hardware Version
			truncation. • Fix CVE-2021-27219: The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.	
2025-05-28	locales	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-1000409 CVE-2018-6485 CVE-2018-11236 CVE-2018-1000001 CVE-2019-9169 CVE-2019-25013 CVE-2020-1752 CVE-2020-10029 CVE-2020-27618	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module • Non-maintainer upload by the ELTS Team. • BZ18036 denial of service in fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS Team. • Backport much of the test support	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219	infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free • CVE-2017-15670 glob buffer overflow • CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow • CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer overflow • CVE-2020-27618 iconv infinite loop • CVE-2020-29573 printf buffer overflow for non-canonical nans • CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for	

Date	Package	CVE(s)	Synopsis	Hardware Version
			getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	
2025-05-28	libc-bin	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-1000409 CVE-2018-6485 CVE-2018-11236 CVE-2018-1000001 CVE-2019-9169 CVE-2019-25013 CVE-2020-1752	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module • Non-maintainer upload by the ELTS Team. • BZ18036 denial of service in fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		CVE-2020-10029 CVE-2020-27618 CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219	Team. • Backport much of the test support infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free • CVE-2017-15670 glob buffer overflow • CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow • CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer overflow • CVE-2020-27618 iconv infinite loop • CVE-2020-29573 printf buffer overflow for non-canonical nans	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	
2025-05-28	libc6	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-1000409 CVE-2018-6485 CVE-2018-11236 CVE-2018-1000001 CVE-2019-9169	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module • Non-maintainer upload by the ELTS Team. • BZ18036 denial of service in	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		CVE-2019-25013 CVE-2020-1752 CVE-2020-10029 CVE-2020-27618 CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219	fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS Team. • Backport much of the test support infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free • CVE-2017-15670 glob buffer overflow • CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow • CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer overflow • CVE-2020-27618 iconv infinite loop	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• CVE-2020-29573 printf buffer overflow for non-canonical nans • CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	
2025-05-28	multiarch-support	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961 CVE-2015-8984 CVE-2017-12132 CVE-2017-12133 CVE-2017-15670 CVE-2017-15671 CVE-2017-15804 CVE-2017-16997 CVE-2017-1000408 CVE-2017-1000409 CVE-2018-6485 CVE-2018-11236 CVE-2018-	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module • Non-maintainer upload by the ELTS	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		1000001 CVE-2019-9169 CVE-2019-25013 CVE-2020-1752 CVE-2020-10029 CVE-2020-27618 CVE-2020-29573 CVE-2021-3326 CVE-2021-3999 CVE-2021-33574 CVE-2021-35942 CVE-2022-23218 CVE-2022-23219	Team. • BZ18036 denial of service in fnmatch, similar to CVE-2015-8984 • Non-maintainer upload by the ELTS Team. • Backport much of the test support infrastructure from 2.24. • CVE-2017-12132 dns spoofing via fragmentation • CVE-2017-12133 clntudp_call use after free • CVE-2017-15670 glob buffer overflow • CVE-2017-15671 glob memory leak • CVE-2017-15804 glob buffer overflow • CVE-2017-16997 setuid privilege escalation involving RPATH • CVE-2017-1000408 ld.so amplifiable memory leak • CVE-2017-1000409 ld.so buffer overflow • CVE-2018-6485 and CVE-2018-6551 posix_memalign integer overflow • CVE-2018-11236 32bit realpath buffer overflow • CVE-2018-1000001 getcwd could return a relative path • CVE-2019-9169 regex out of bounds read • CVE-2019-25013 oob read in iconv • CVE-2020-1752 use after free in glob • CVE-2020-10029 sinl buffer	

Date	Package	CVE(s)	Synopsis	Hardware Version
			overflow • CVE-2020-27618 iconv infinite loop • CVE-2020-29573 printf buffer overflow for non-canonical nans • CVE-2021-3326 iconv abort • CVE-2021-3999 oob write for getcwd size 1 • CVE-2021-33574 mq_notify use after free • CVE-2021-35942 wordexp input validation • CVE-2022-23218 svcunix_create buffer overflow • CVE-2022-23219 clnt_create buffer overflow	
2025-05-30	libcurl3	CVE-2023-27534 CVE-2023-27534 CVE-2023-27534 CVE-2023-28321 CVE-2023-28321 CVE-2023-28322 CVE-2023-28322 CVE-2024-7264 CVE-2023-38546 CVE-2023-27533 CVE-2023-27535 CVE-2023-27536 CVE-2023-27538 CVE-2022-27774 CVE-2022-27774 CVE-2022-27782 CVE-2022-	• Non-maintainer upload by the ELTS team. • debian/gbp.conf: add file with minimal settings and debian/jessie default. • debian/patches/: ○ CVE-2023-27534.patch: backport patch to jessie's version. + CVE-2023-27534: SFTP path ~ resolving discrepancy. ○ fix-CVE-2023-27534-regression.patch: add new patch from upstream to restore sftp://host/~ behaviour. ○ CVE-2023-28321.patch: backport patch to jessie's version. + CVE-2023-28321: IDN wildcard match.	M400 M410 R100E R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
		32221 CVE-2022-35252 CVE-2022-43552 CVE-2022-22576 CVE-2022-27776 CVE-2022-27781 CVE-2022-32208 CVE-2021-22946 CVE-2021-22947 CVE-2021-22898	○ CVE-2023-28322.patch: backport patch to jessie's version. + CVE-2023-28322: more POST-after-PUT confusion. • debian/salsa-ci.yml: add ELTS pipeline for jessie. • Non-maintainer upload by the ELTS team. • Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used. • Non-maintainer upload by the ELTS team. • CVE-2023-38546: cookie injection • Non-maintainer upload by the ELTS team. • Fix CVE-2023-27533: A vulnerability in input validation exists in curl during communication using the TELNET protocol may allow an attacker to pass on maliciously crafted user name and "telnet options" during server negotiation. The lack of proper input scrubbing allows an attacker to send content or perform option negotiation without the application's intent. This vulnerability could be exploited if an application allows user input,	

Date	Package	CVE(s)	Synopsis	Hardware Version
			thereby enabling attackers to execute arbitrary code on the system. • Fix CVE-2023-27535: An authentication bypass vulnerability exists in libcurl in the FTP connection reuse feature that can result in wrong credentials being used during subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current setup. However, certain FTP settings such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_USE_SSL were not included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong credentials when performing a transfer, potentially allowing unauthorized access to sensitive information. • CVE-2023-27536: An authentication bypass vulnerability exists in libcurl in the connection reuse feature which can reuse previously established connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This vulnerability affects krb5/kerberos/negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest option is to not reuse connections if the CURLOPT_GSSAPI_DELEGATION option has been changed. • Fix CVE-2023-27538: An authentication bypass vulnerability exists in libcurl where it reuses a	

Date	Package	CVE(s)	Synopsis	Hardware Version
			previously established SSH connection despite the fact that an SSH option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections to reuse them for subsequent transfers if the configurations match. However, two SSH settings were omitted from the configuration check, allowing them to match easily, potentially leading to the reuse of an inappropriate connection. • Follow up to CVE-2022-27774: The patch included to address this CVE in 7.38.0-4+deb8u24 contained a defect which could result in a segmentation fault and application crash. The patch is corrected in this update. • Non-maintainer upload by the ELTS Team. • CVE-2022-27774: An insufficiently protected credentials vulnerability exists in curl that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different protocols or port numbers. • CVE-2022-27782: libcurl would reuse a previously created connection even when a TLS or SSH related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, several TLS and SSH settings were left out from the	

Date	Package	CVE(s)	Synopsis	Hardware Version
			configuration match checks, making them match too easily. • CVE-2022-32221: When doing HTTP(S) transfers, libcurl might erroneously use the read callback (CURLOPT_READFUNCTION) to ask for data to send, even when the CURLOPT_POSTFIELDS option has been set, if the same handle previously was used to issue a PUT request which used that callback. • CVE-2022-35252: When curl is used to retrieve and parse cookies from a HTTP(S) server, it accepts cookies using control codes that when later are sent back to a HTTP server might make the server return 400 responses. Effectively allowing a "sister site" to deny service to all siblings. • CVE-2022-43552: HTTP Proxy deny use-after-free • Non-maintainer upload by the ELTS team. • Fix CVE-2022-22576: An improper authentication vulnerability exists in curl which might allow reuse OAUTH2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMPTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only). • Fix CVE-2022-27776: A insufficiently protected credentials vulnerability in curl might leak authentication or cookie header data on HTTP redirects to the same host but another port number.	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• Fix CVE-2022-27781: libcurl provides the CURLOPT_CERTINFO option to allow applications to request details to be returned about a server's certificate chain. Due to an erroneous function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation. • Fix CVE-2022-32208: When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client. • Non-maintainer upload by the ELTS Team. • CVE-2021-22946 Crafted answers from a server might force clients to not use TLS on connections though TLS was required and expected. • CVE-2021-22947 When using STARTTLS to initiate a TLS connection, the server might send multiple answers before the TLS upgrade and such the client would handle them as being trusted. This could be used by a MITM-attacker to inject fake response data. • Non-maintainer upload by the ELTS team. • CVE-2021-22898: Information disclosure in connection to telnet servers.	
2025-05-30	curl	CVE-2023-27534 CVE-2023-27534	• Non-maintainer upload by the ELTS team.	M400 M410 R100E

Date	Package	CVE(s)	Synopsis	Hardware Version
		CVE-2023-27534 CVE-2023-28321 CVE-2023-28321 CVE-2023-28322 CVE-2023-28322 CVE-2024-7264 CVE-2023-38546 CVE-2023-27533 CVE-2023-27535 CVE-2023-27536 CVE-2023-27538 CVE-2022-27774 CVE-2022-27774 CVE-2022-27782 CVE-2022-32221 CVE-2022-35252 CVE-2022-43552 CVE-2022-22576 CVE-2022-27776 CVE-2022-27781 CVE-2022-32208 CVE-2021-22946 CVE-2021-22947 CVE-2021-22898	• debian/gbp.conf: add file with minimal settings and debian/jessie default. • debian/patches/: ○ CVE-2023-27534.patch: backport patch to jessie's version. + CVE-2023-27534: SFTP path ~ resolving discrepancy. ○ fix-CVE-2023-27534-regression.patch: add new patch from upstream to restore sftp://host/~ behaviour. ○ CVE-2023-28321.patch: backport patch to jessie's version. + CVE-2023-28321: IDN wildcard match. ○ CVE-2023-28322.patch: backport patch to jessie's version. + CVE-2023-28322: more POST-after-PUT confusion. • debian/salsa-ci.yml: add ELTS pipeline for jessie. • Non-maintainer upload by the ELTS team. • Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the	R100NA S1600E S100

Date	Package	CVE(s)	Synopsis	Hardware Version
			application when CURLINFO_CERTINFO is used. • Non-maintainer upload by the ELTS team. • CVE-2023-38546: cookie injection • Non-maintainer upload by the ELTS team. • Fix CVE-2023-27533: A vulnerability in input validation exists in curl during communication using the TELNET protocol may allow an attacker to pass on maliciously crafted user name and "telnet options" during server negotiation. The lack of proper input scrubbing allows an attacker to send content or perform option negotiation without the application's intent. This vulnerability could be exploited if an application allows user input, thereby enabling attackers to execute arbitrary code on the system. • Fix CVE-2023-27535: An authentication bypass vulnerability exists in libcurl in the FTP connection reuse feature that can result in wrong credentials being used during subsequent transfers. Previously created connections are kept in a connection pool for reuse if they match the current setup. However, certain FTP settings such as CURLOPT_FTP_ACCOUNT, CURLOPT_FTP_ALTERNATIVE_TO_USER, CURLOPT_FTP_SSL_CCC, and CURLOPT_USE_SSL were not included in the configuration match checks, causing them to match too easily. This could lead to libcurl using the wrong credentials when performing a transfer, potentially	

Date	Package	CVE(s)	Synopsis	Hardware Version
			allowing unauthorized access to sensitive information. • CVE-2023-27536: An authentication bypass vulnerability exists in libcurl in the connection reuse feature which can reuse previously established connections with incorrect user permissions due to a failure to check for changes in the CURLOPT_GSSAPI_DELEGATION option. This vulnerability affects krb5/kerberos/negotiate/GSSAPI transfers and could potentially result in unauthorized access to sensitive information. The safest option is to not reuse connections if the CURLOPT_GSSAPI_DELEGATION option has been changed. • Fix CVE-2023-27538: An authentication bypass vulnerability exists in libcurl where it reuses a previously established SSH connection despite the fact that an SSH option was modified, which should have prevented reuse. libcurl maintains a pool of previously used connections to reuse them for subsequent transfers if the configurations match. However, two SSH settings were omitted from the configuration check, allowing them to match easily, potentially leading to the reuse of an inappropriate connection. • Follow up to CVE-2022-27774: The patch included to address this CVE in 7.38.0-4+deb8u24 contained a defect which could result in a segmentation fault and application crash. The patch is corrected in this update. • Non-maintainer upload by the ELTS	

Date	Package	CVE(s)	Synopsis	Hardware Version
			Team. • CVE-2022-27774: An insufficiently protected credentials vulnerability exists in curl that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different protocols or port numbers. • CVE-2022-27782: libcurl would reuse a previously created connection even when a TLS or SSH related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, several TLS and SSH settings were left out from the configuration match checks, making them match too easily. • CVE-2022-32221: When doing HTTP(S) transfers, libcurl might erroneously use the read callback (CURLOPT_READFUNCTION) to ask for data to send, even when the CURLOPT_POSTFIELDS option has been set, if the same handle previously was used to issue a PUT request which used that callback. • CVE-2022-35252: When curl is used to retrieve and parse cookies from a HTTP(S) server, it accepts cookies using control codes that when later are sent back to a HTTP server might make the server return 400 responses. Effectively allowing a "sister site" to deny service to all siblings. • CVE-2022-43552: HTTP Proxy deny	

Date	Package	CVE(s)	Synopsis	Hardware Version
			use-after-free • Non-maintainer upload by the ELTS team. • Fix CVE-2022-22576: An improper authentication vulnerability exists in curl which might allow reuse OAUTH2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMPTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only). • Fix CVE-2022-27776: A insufficiently protected credentials vulnerability in curl might leak authentication or cookie header data on HTTP redirects to the same host but another port number. • Fix CVE-2022-27781: libcurl provides the CURLOPT_CERTINFO option to allow applications to request details to be returned about a server's certificate chain. Due to an erroneous function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation. • Fix CVE-2022-32208: When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client. • Non-maintainer upload by the ELTS Team.	

Date	Package	CVE(s)	Synopsis	Hardware Version
			• CVE-2021-22946 Crafted answers from a server might force clients to not use TLS on connections though TLS was required and expected. • CVE-2021-22947 When using STARTTLS to initiate a TLS connection, the server might send multiple answers before the TLS upgrade and such the client would handle them as being trusted. This could be used by a MITM-attacker to inject fake response data. • Non-maintainer upload by the ELTS team. • CVE-2021-22898: Information disclosure in connection to telnet servers.	
2025-05-31	net-tools	CVE-2025-46836	• Non-maintainer upload by the ELTS Team. • CVE-2025-46836: interface.c: Stack-based Buffer Overflow in get_name() • ipmaddr.c: Stack-based buffer Overflow in parse_hex() • proc.c: Stack-based Buffer Overflow in proc_gen_fmt()	M400 M410 R100E R100NA S1600E S100
2025-06-14	libicu52	CVE-2025-5222 CVE-2020-21913	• Non-maintainer upload by the ELTS Team. • CVE-2025-5222: Stack-based buffer overflow • Non-maintainer upload by the LTS team. • CVE-2020-21913: Prevent a potential use-after-free vulnerability in the pkg_createWithAssemblyCode function.	M400 M410 R100E R100NA S1600E S100

Unified v2.9.3 Security Updates

This table describes the security updates available for Unified v2.9.3 base stations since the last update, through **2025-06-30**.

Date	Package	CVE(s)	Synopsis	Hardware Version
2025-05-26	krb5-locales	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	
2025-05-26	libk5crypto3	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	

Date	Package	CVE(s)	Synopsis	Hardware Version
2025-05-26	libglib2.0-data	CVE-2025-4373 CVE-2024-52533 CVE-2024-34397	• Non-maintainer upload by the ELTS team. • Fix CVE-2025-4373: A flaw was found in GLib, which is vulnerable to an integer overflow in the g_string_insert_unichar() function. When the position at which to insert the character is large, the position will overflow, leading to a buffer underwrite. • Add patch and define the inline keyword in gmem.h to avoid FTBFS in reverse-dependencies which require the header file. • Non-maintainer upload by the ELTS Team. • CVE-2024-52533: SOCKS4a proxy buffer overflow • Non-maintainer upload the ELTS team. • Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact.	M400 S1600E M410 R100E S100 R100NA
2025-05-26	libgssapi-krb5-2	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in	

Date	Package	CVE(s)	Synopsis	Hardware Version
			gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	
2025-05-26	libkrb5-3	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype()	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated tokens	
2025-05-26	libkrb5support0	CVE-2025-3576 CVE-2024-26462 CVE-2024-26458 CVE-2024-26461 CVE-2024-37370 CVE-2024-37371	• Non Maintainer upload by the ELTS team • Fix CVE-2025-3576. A Vulnerability in the MIT Kerberos implementation allows GSSAPI-protected messages using RC4-HMAC-MD5 to be spoofed due to weaknesses in the MD5 checksum design. If RC4 is preferred over stronger encryption types, an attacker could exploit MD5 collisions to forge message integrity codes. This may lead to unauthorized message tampering. • Because of the possibility of breaking certain older authentication systems, the	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			configuration variables which have been introduced as part of the fix (allow_rc4 and allow_des3) are treated as 'true' by default. This leaves the 3DES and RC4 algorithms enabled, but administrators are strongly encouraged to disable them after verifying compatibility in their environments. • In KDC, assume all services support aes256-sha1 To facilitate negotiating session keys with acceptable security, assume that services support aes256-cts-hmac-sha1 unless a session_enctypes string attribute says otherwise. • Add krb5int_c_deprecated_enctype() checks for the ETYPE_DEPRECATED flag on enctypes. All ENCTYPE_WEAK enctypes are currently deprecated; not all deprecated enctypes are considered weak. Deprecations follow RFC 6649 and RFC 8429. • Non Maintainer upload by LTS team • Fixes CVE-2024-26462 A memory leak vulnerability was found in /krb5/src/kdc/ndr.c. • Non-maintainer upload by the ELTS Team. • CVE-2024-26458: Memory leak in xmt_rmtcallres() • CVE-2024-26461: Memory leak in gss_krb5int_make_seal_token_v3() • CVE-2024-37370: GSS wrap token Extra Count field manipulation • CVE-2024-37371: Invalid GSS memory reads with manipulated	

Date	Package	CVE(s)	Synopsis	Hardware Version
			tokens	
2025-05-26	libglib2.0-0	CVE-2025-4373 CVE-2024-52533 CVE-2024-34397	• Non-maintainer upload by the ELTS team. • Fix CVE-2025-4373: A flaw was found in GLib, which is vulnerable to an integer overflow in the g_string_insert_unichar() function. When the position at which to insert the character is large, the position will overflow, leading to a buffer underwrite. • Add patch and define the inline keyword in gmem.h to avoid FTBFS in reverse-dependencies which require the header file. • Non-maintainer upload by the ELTS Team. • CVE-2024-52533: SOCKS4a proxy buffer overflow • Non-maintainer upload the ELTS team. • Fix CVE-2024-34397: Alicia Boya Garcia reported that the GDBus signal subscriptions in the GLib library are prone to a spoofing vulnerability. A local attacker can take advantage of this flaw to cause a GDBus-based client to behave incorrectly, with an application-dependent impact.	M400 S1600E M410 R100E S100 R100NA
2025-05-28	locales	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team.	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
		2961	• CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	
2025-05-28	libc-bin	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
2025-05-28	libc6	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	M400 S1600E M410 R100E S100 R100NA
2025-05-28	multiarch-support	CVE-2025-0395 CVE-2025-0395 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-2961	• Non-maintainer upload by the ELTS Team. • debian/patches/local-CVE-2025-0395-{1,2}.diff: Fix buffer overflow in assert() function (CVE-2025-0395). • Non-maintainer upload by the ELTS Team. • CVE-2024-33599: nscd: Stack-based buffer overflow in netgroup cache • CVE-2024-33600: nscd: Null pointer crashes after notfound response • CVE-2024-33601: nscd: Daemon may terminate on memory	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			allocation failure • CVE-2024-33602: nscd: Possible memory corruption • Non-maintainer upload by the ELTS Team. • CVE-2024-2961: Out-of-bounds write in iconv ISO-2022-CN-EXT module	
2025-05-30	libcurl3	CVE-2023-27534 CVE-2023-27534 CVE-2023-27534 CVE-2023-28321 CVE-2023-28321 CVE-2023-28322 CVE-2023-28322 CVE-2024-7264	• Non-maintainer upload by the ELTS team. • debian/gbp.conf: add file with minimal settings and debian/jessie default. • debian/patches/: ○ CVE-2023-27534.patch: backport patch to jessie's version. + CVE-2023-27534: SFTP path ~ resolving discrepancy. ○ fix-CVE-2023-27534-regression.patch: add new patch from upstream to restore sftp://host/~ behaviour. ○ CVE-2023-28321.patch: backport patch to jessie's version. + CVE-2023-28321: IDN wildcard match. ○ CVE-2023-28322.patch: backport patch to jessie's version. + CVE-2023-28322: more POST-after-PUT confusion. • debian/salsa-ci.yml: add ELTS pipeline for jessie. • Non-maintainer upload by the ELTS	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			team. • Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used.	
2025-05-30	curl	CVE-2023-27534 CVE-2023-27534 CVE-2023-27534 CVE-2023-28321 CVE-2023-28321 CVE-2023-28322 CVE-2023-28322 CVE-2024-7264	• Non-maintainer upload by the ELTS team. • debian/gbp.conf: add file with minimal settings and debian/jessie default. • debian/patches/: ○ CVE-2023-27534.patch: backport patch to jessie's version. + CVE-2023-27534: SFTP path ~ resolving discrepancy. ○ fix-CVE-2023-27534-regression.patch: add new patch from upstream to restore sftp://host/~ behaviour. ○ CVE-2023-28321.patch: backport patch to jessie's version. + CVE-2023-28321: IDN wildcard match. ○ CVE-2023-28322.patch: backport patch to jessie's version. + CVE-2023-28322: more POST-after-PUT	M400 S1600E M410 R100E S100 R100NA

Date	Package	CVE(s)	Synopsis	Hardware Version
			confusion. • debian/salsa-ci.yml: add ELTS pipeline for jessie. • Non-maintainer upload by the ELTS team. • Fix CVE-2024-7264: A denial-of-service vulnerability was found in cURL, an easy-to-use client-side URL transfer library. libcurl's ASN1 parser code has the GTime2str() function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up crashing but this flaw can also lead to heap contents getting returned to the application when CURLINFO_CERTINFO is used.	
2025-05-31	net-tools	CVE-2025-46836	• Non-maintainer upload by the ELTS Team. • CVE-2025-46836: interface.c: Stack-based Buffer Overflow in get_name() • ipmaddr.c: Stack-based buffer Overflow in parse_hex() • proc.c: Stack-based Buffer Overflow in proc_gen_fmt()	M400 S1600E M410 R100E S100 R100NA
2025-06-14	libicu52	CVE-2025-5222	• Non-maintainer upload by the ELTS Team. • CVE-2025-5222: Stack-based buffer overflow	M400 S1600E M410 R100E S100 R100NA