Security Export

SCA scan: DONE, Fri May 30, 2025

Contextual Analysis scan: DONE, Fri May 30, 2025

Exported on: Fri May 30, 2025

Exported by: breezin_ahimusa@aol.com

Package type: Docker

Sha256: ac6e323dffe6addce0d4ed9aa5a8e86ae926a7a2c26e51b59e0d6e9a2a942be1

Component name: spring-petclinic:latest

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1.18.26 is prone to a directory traversal vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debian.tar, the in-place extraction can lead to directory traversal situations on specially crafted orig.tar and debian.tar tarballs.	CVE-2022-1664	Critical	Medium		debian:bullseye:dpkg	< 1.20.10	1.20.10	2022-09-04T15:24:00Z	Applicable
A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.	CVE-2023-4911	High	High		debian:bullseye:libc-bin	< 2.31-13+deb11u7	2.31-13+deb11u7	0001-01-01T00:00:00Z	Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.	CVE-2023-4911	High	High		debian:bullseye:libc6	< 2.31-13+deb11u7	2.31-13+deb11u7	0001-01-01T00:00:00Z	Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability

Path Equivalence: 'file.Name' (Internal Dot) leading toÂ Remote Code Execution and/or Information disclosureÂ and/or malicious content added to uploaded files via write enabledÂ Default ServletÂ in Apache Tomcat.
 	
This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.2, from 10.1.0-M1 through 10.1.34, from 9.0.0.M1 through 9.0.98.
 	
If all of the following were true, a malicious user was able to view security sensitive files and/or inject content into those files:
-Â writes enabled for the default servlet (disabled by default)
- support for partial PUT (enabled by default)
- a target URL for security sensitive uploads that was a sub-directory ofÂ a target URL for public uploads
-Â attacker knowledge of the names of security sensitive files
beingÂ uploaded
-Â the security sensitive files also being uploaded via partial PUT
 	
If all of the following were true, a malicious user was able to perform remote code execution:
- writes enabled for the default servlet (disabled by default)
-Â support for partial PUT (enabled by default)
-Â application was using Tomcat's file based session persistence with
theÂ default storage location
	CVE-2025-24813	Critical	High	sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/BOOT-INF/lib/tomcat-embed-core-10.1.34.jar;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav://org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav://org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34
					org.apache.tomcat.embed:tomcat-embed-core	10.1.0-M1 <= Version < 10.1.35,11.0.0-M1 <= Version < 11.0.3,9.0.0.M1 <= Version < 9.0.99	10.1.35,11.0.3,9.0.99	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
-Â application included a library that may be leveraged in aÂ deserialization attack Users are recommended to upgrade to version 11.0.3, 10.1.35 or 9.0.99, which fixes the issue.									
MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in zipOpenNewFileInZip4_64 via a long filename, comment, or extra field. NOTE: MiniZip is not a supported part of the zlib product. NOTE: pyminizip through 0.2.6 is also vulnerable because it bundles an affected zlib version, and exposes the applicable MiniZip code through its compress API.	CVE-2023-45853	Critical	High		debian:bullseye:zlib1g	All Versions		0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field. NOTE: only applications that call inflateGetHeader are affected. Some common applications bundle the affected zlib source code but may be unable to call inflateGetHeader (e.g., see the nodejs/node reference).	CVE-2022-37434	Critical	High		debian:bullseye:zlib1g	< 1:1.2.11.dfsg-2+deb11u2	1:1.2.11.dfsg-2+deb11u2	2023-01-08T19:26:00Z	Not Applicable
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause invalid memory reads during GSS message token handling by sending message tokens with invalid length fields.	CVE-2024-37371	Critical	Medium		debian:bullseye:libgssapi-krb5-2	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause invalid memory reads during GSS message token handling by sending message tokens with invalid length fields.	CVE-2024-37371	Critical	Medium		debian:bullseye:libk5crypto3	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause invalid memory reads during GSS message token handling by sending message tokens with invalid length fields.	CVE-2024-37371	Critical	Medium		debian:bullseye:libkrb5support0	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can cause invalid memory reads during GSS message token handling by sending message tokens with invalid length fields.	CVE-2024-37371	Critical	Medium		debian:bullseye:libkrb5-3	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable
GNU Libtasn1 before 4.19.0 has an ETYPE_OK off-by-one array size check that affects asn1_encode_simple_der.	CVE-2021-46848	Critical	Medium		debian:bullseye:libtasn1-6	< 4.16.0-2+deb11u1	4.16.0-2+deb11u1	2023-06-04T16:26:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).	CVE-2022-2068	Critical	Medium		debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u3	1.1.1n-0+deb11u3	2023-01-08T19:26:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).	CVE-2022-2068	Critical	Medium		debian:bullseye:openssl	< 1.1.1n-0+deb11u3	1.1.1n-0+deb11u3	2023-01-08T19:26:00Z	Not Applicable

			JFrog			Infected	Fix		
Summary	CVEs	Severity	Severity	Component Physical Paths	Component	Version	Version	Edited	Applicability
The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).	CVE-2022-1292	Critical	Medium		debian:bullseye:libssl1.1	0:1.0.2 <= Version < 0:1.0.2ze,0:1.1.1 <= Version < 1.1.1n-0+deb11u2,0:3.0.0 <= Version < 0:3.0.3	1.1.1n-0+deb11u2	2022-12-22T09:25:00Z	Not Applicable
The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).	CVE-2022-1292	Critical	Medium		debian:bullseye:openssl	0:1.0.2 <= Version < 0:1.0.2ze,0:1.1.1 <= Version < 1.1.1n-0+deb11u2,0:3.0.0 <= Version < 0:3.0.3	1.1.1n-0+deb11u2	2022-12-22T09:25:00Z	Not Applicable
SQLite3 from 3.6.0 to and including 3.27.2 is vulnerable to heap out-of-bound read in the rtreenode() function when handling invalid rtree tables.	CVE-2019-8457	Critical	Low		debian:bullseye:libdb5.3	All Versions		2022-11-23T20:19:00Z	Not Applicable

			JFrog			Infected	Fix		
Summary	CVEs	Severity	Severity	Component Physical Paths	Component	Version	Version	Edited	Applicability
An out-of-bounds read vulnerability was discovered in the PCRE2 library in the get_recurse_data_length() function of the pcre2_jit_compile.c file. This issue affects recursions in JIT-compiled regular expressions caused by duplicate data transfers.	CVE-2022-1587	Critical	Low		debian:bullseye:libpcre2-8-0	< 10.36-2+deb11u1	10.36-2+deb11u1	2023-01-08T19:25:00Z	Not Applicable
An out-of-bounds read vulnerability was discovered in the PCRE2 library in the compile_xclass_matchingpath() function of the pcre2_jit_compile.c file. This involves a unicode property matching issue in JIT-compiled regular expressions. The issue occurs because the character was not fully read in case-less matching within JIT.	CVE-2022-1586	Critical	Low		debian:bullseye:libpcre2-8-0	< 10.36-2+deb11u1	10.36-2+deb11u1	2023-01-08T19:25:00Z	Not Applicable

Improper Neutralization of Escape, Meta, or Control Sequences vulnerability in Apache Tomcat.Â For a subset of unlikely rewrite rule configurations, it was possible for a specially crafted request to bypass some rewrite rules. If those rewrite rules effectively enforced security constraints, those constraints could be bypassed.
This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.5, from 10.1.0-M1 through 10.1.39, from 9.0.0.M1 through 9.0.102.
Users are recommended to upgrade to version [FIXED_VERSION], which fixes the issue.
	CVE-2025-31651	Critical		sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/BOOT-INF/lib/tomcat-embed-core-10.1.34.jar
					org.apache.tomcat.embed:tomcat-embed-core	10.1.10 <= Version < 10.1.40,11.0.0-M2 <= Version < 11.0.6,9.0.76 <= Version <= 9.0.102	10.1.40,11.0.6,9.0.104	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A vulnerability was found in GnuTLS. The response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from the response times of ciphertexts with correct PKCS#1 v1.5 padding. This issue may allow a remote attacker to perform a timing side-channel attack in the RSA-PSK key exchange, potentially leading to the leakage of sensitive data. CVE-2024-0553 is designated as an incomplete resolution for CVE-2023-5981.	CVE-2024-0553	High	High		debian:bullseye:libgnutls30	< 3.7.1-5+deb11u5	3.7.1-5+deb11u5	0001-01-01T00:00:00Z	Not Applicable
A timing side-channel in the handling of RSA ClientKeyExchange messages was discovered in GnuTLS. This side-channel can be sufficient to recover the key encrypted in the RSA ciphertext across a network in a Bleichenbacher style attack. To achieve a successful decryption the attacker would need to send a large amount of specially crafted messages to the vulnerable server. By recovering the secret from the ClientKeyExchange message, the attacker would be able to decrypt the application data exchanged over that connection.	CVE-2023-0361	High	High		debian:bullseye:libgnutls30	< 3.7.1-5+deb11u3	3.7.1-5+deb11u3	2023-05-11T13:04:00Z	Not Applicable
PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may lead to remote code execution (in KDC, kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer overflow), and cause a denial of service on other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has "a similar bug."	CVE-2022-42898	High	High		debian:bullseye:libkrb5support0	< 1.18.3-6+deb11u3	1.18.3-6+deb11u3	2023-02-15T12:36:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may lead to remote code execution (in KDC, kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer overflow), and cause a denial of service on other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has "a similar bug."	CVE-2022-42898	High	High		debian:bullseye:libk5crypto3	< 1.18.3-6+deb11u3	1.18.3-6+deb11u3	2023-02-15T12:36:00Z	Not Applicable
PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may lead to remote code execution (in KDC, kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer overflow), and cause a denial of service on other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has "a similar bug."	CVE-2022-42898	High	High		debian:bullseye:libgssapi-krb5-2	< 1.18.3-6+deb11u3	1.18.3-6+deb11u3	2023-02-15T12:36:00Z	Not Applicable
PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may lead to remote code execution (in KDC, kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer overflow), and cause a denial of service on other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has "a similar bug."	CVE-2022-42898	High	High		debian:bullseye:libkrb5-3	< 1.18.3-6+deb11u3	1.18.3-6+deb11u3	2023-02-15T12:36:00Z	Not Applicable

			JFrog			Infected	Fix		
Summary	**CVEs**	**Severity**	**Severity**	**Component Physical Paths**	**Component**	**Version**	**Version**	**Edited**	**Applicability**
An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system.	CVE-2022-1271	High	High		debian:bullseye:liblzma5	< 5.2.5-2.1~deb11u1	5.2.5-2.1~deb11u1	2023-02-15T12:36:00Z	Not Applicable
An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system.	CVE-2022-1271	High	High		debian:bullseye:gzip	< 1.10-4+deb11u1	1.10-4+deb11u1	2023-02-15T12:36:00Z	Not Applicable
CPAN 2.28 allows Signature Verification Bypass.	CVE-2020-16156	High	High		debian:bullseye:perl-base	< 5.32.1-4+deb11u4	5.32.1-4+deb11u4	2023-02-25T21:26:00Z	Not Applicable
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the plaintext Extra Count field of a confidential GSS krb5 wrap token, causing the unwrapped token to appear truncated to the application.	CVE-2024-37370	High	Medium		debian:bullseye:libkrb5-3	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the plaintext Extra Count field of a confidential GSS krb5 wrap token, causing the unwrapped token to appear truncated to the application.	CVE-2024-37370	High	Medium		debian:bullseye:libk5crypto3	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the plaintext Extra Count field of a confidential GSS krb5 wrap token, causing the unwrapped token to appear truncated to the application.	CVE-2024-37370	High	Medium		debian:bullseye:libkrb5support0	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable
In MIT Kerberos 5 (aka krb5) before 1.21.3, an attacker can modify the plaintext Extra Count field of a confidential GSS krb5 wrap token, causing the unwrapped token to appear truncated to the application.	CVE-2024-37370	High	Medium		debian:bullseye:libgssapi-krb5-2	< 1.18.3-6+deb11u5	1.18.3-6+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.	CVE-2023-0286	High	Medium		debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-03-07T11:40:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address field as ASN1_TYPE. This field is subsequently interpreted by the OpenSSL function GENERAL_NAME_cmp as an ASN1_TYPE rather than an ASN1_STRING. When CRL checking is enabled (i.e. the application sets the X509_V_FLAG_CRL_CHECK flag), this vulnerability may allow an attacker to pass arbitrary pointers to a memcmp call, enabling them to read memory contents or enact a denial of service. In most cases, the attack requires the attacker to provide both the certificate chain and CRL, neither of which need to have a valid signature. If the attacker only controls one of these inputs, the other input must already contain an X.400 address as a CRL distribution point, which is uncommon. As such, this vulnerability is most likely to only affect applications which have implemented their own functionality for retrieving CRLs over a network.	CVE-2023-0286	High	Medium		debian:bullseye:openssl	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-03-07T11:40:00Z	Not Applicable

			JFrog			Infected	Fix		
Summary	CVEs	Severity	Severity	Component Physical Paths	Component	Version	Version	Edited	Applicability
The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call	CVE-2023-0215	High	Medium		debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-03-19T08:11:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.		🟥	🟧						

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The public API function BIO_new_NDEF is a helper function used for streaming ASN.1 data via a BIO. It is primarily used internally to OpenSSL to support the SMIME, CMS and PKCS7 streaming capabilities, but may also be called directly by end user applications. The function receives a BIO from the caller, prepends a new BIO_f_asn1 filter BIO onto the front of it to form a BIO chain, and then returns the new head of the BIO chain to the caller. Under certain conditions, for example if a CMS recipient public key is invalid, the new filter BIO is freed and the function returns a NULL result indicating a failure. However, in this case, the BIO chain is not properly cleaned up and the BIO passed by the caller still retains internal pointers to the previously freed filter BIO. If the caller then goes on to call BIO_pop() on the BIO then a use-after-free will occur. This will most likely result in a crash. This scenario occurs directly in the internal function B64_write_ASN1() which may cause BIO_new_NDEF() to be called and will subsequently call	CVE-2023-0215	High	Medium		debian:bullseye:openssl	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-03-19T08:11:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
BIO_pop() on the BIO. This internal function is in turn called by the public API functions PEM_write_bio_ASN1_stream, PEM_write_bio_CMS_stream, PEM_write_bio_PKCS7_stream, SMIME_write_ASN1, SMIME_write_CMS and SMIME_write_PKCS7. Other public API functions that may be impacted by this include i2d_ASN1_bio_stream, BIO_new_CMS, BIO_new_PKCS7, i2d_CMS_bio_stream and i2d_PKCS7_bio_stream. The OpenSSL cms and smime command line applications are similarly affected.		🟥	🟧						

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data. If the function succeeds then the "name_out", "header" and "data" arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including	CVE-2022-4450	High	Medium		debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-05-17T12:30:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue.		🟥	🟧						

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The function PEM_read_bio_ex() reads a PEM file from a BIO and parses and decodes the "name" (e.g. "CERTIFICATE"), any header data and the payload data. If the function succeeds then the "name_out", "header" and "data" arguments are populated with pointers to buffers containing the relevant decoded data. The caller is responsible for freeing those buffers. It is possible to construct a PEM file that results in 0 bytes of payload data. In this case PEM_read_bio_ex() will return a failure code but will populate the header argument with a pointer to a buffer that has already been freed. If the caller also frees this buffer then a double free will occur. This will most likely lead to a crash. This could be exploited by an attacker who has the ability to supply malicious PEM files for parsing to achieve a denial of service attack. The functions PEM_read_bio() and PEM_read() are simple wrappers around PEM_read_bio_ex() and therefore these functions are also directly affected. These functions are also called indirectly by a number of other OpenSSL functions including	CVE-2022-4450	High	Medium		debian:bullseye:openssl	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-05-17T12:30:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
PEM_X509_INFO_read_bio_ex() and SSL_CTX_use_serverinfo_file() which are also vulnerable. Some OpenSSL internal uses of these functions are not vulnerable because the caller does not free the header argument if PEM_read_bio_ex() returns a failure code. These locations include the PEM_read_bio_TYPE() functions as well as the decoders introduced in OpenSSL 3.0. The OpenSSL asn1parse command line application is also impacted by this issue.									
Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address a side-channel attack against mpi_powm, and the window size is not chosen appropriately. This, for example, affects use of ElGamal in OpenPGP.	CVE-2021-33560	High	Medium		debian:bullseye:libgcrypt20	All Versions		2023-02-26T14:02:00Z	Not Applicable
A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTLS) rejects a certificate chain with distributed trust. This issue occurs when validating a certificate chain with cockpit-certificate-ensure. This flaw allows an unauthenticated, remote client or attacker to initiate a denial of service attack.	CVE-2024-0567	High	Low		debian:bullseye:libgnutls30	< 3.7.1-5+deb11u5	3.7.1-5+deb11u5	0001-01-01T00:00:00Z	Not Applicable
A vulnerability was found in perl 5.30.0 through 5.38.0. This issue occurs when a crafted regular expression is compiled by perl, which can allow an attacker controlled byte buffer overflow in a heap allocated buffer.	CVE-2023-47038	High	Low		debian:bullseye:perl-base	< 5.32.1-4+deb11u3	5.32.1-4+deb11u3	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.	CVE-2023-29491	High	Low		debian:bullseye:ncurses-base	< 6.2+20201114-2+deb11u2	6.2+20201114-2+deb11u2	0001-01-01T00:00:00Z	Not Applicable
ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.	CVE-2023-29491	High	Low		debian:bullseye:libtinfo6	< 6.2+20201114-2+deb11u2	6.2+20201114-2+deb11u2	0001-01-01T00:00:00Z	Not Applicable
ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.	CVE-2023-29491	High	Low		debian:bullseye:ncurses-bin	< 6.2+20201114-2+deb11u2	6.2+20201114-2+deb11u2	0001-01-01T00:00:00Z	Not Applicable
A vulnerability was found in zstd v1.4.10, where an attacker can supply empty string as an argument to the command line tool to cause buffer overrun.	CVE-2022-4899	High	Low		debian:bullseye:libzstd1	All Versions		2023-05-14T11:37:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability

Improper Input Validation vulnerability in Apache Tomcat. Incorrect error handling for some invalid HTTP priority headers resulted in incomplete clean-up of the failed request which created a memory leak. A large number of such requests could trigger an OutOfMemoryException resulting in a denial of service.
 	
This issue affects Apache Tomcat: from 9.0.76 through 9.0.102, from 10.1.10 through 10.1.39, from 11.0.0-M2 through 11.0.5.
 	
Users are recommended to upgrade to version 9.0.104, 10.1.40 or 11.0.6 which fix the issue.
	CVE-2025-31650	High		sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/BOOT-INF/lib/tomcat-embed-core-10.1.34.jar
					org.apache.tomcat.embed:tomcat-embed-core	10.1.10 <= Version < 10.1.40,11.0.0-M2 <= Version < 11.0.6,9.0.76 <= Version <= 9.0.102	10.1.40,11.0.6,9.0.104	0001-01-01T00:00:00Z	Not Applicable

			JFrog			Infected	Fix		
Summary	CVEs	Severity	Severity	Component Physical Paths	Component	Version	Version	Edited	Applicability

EndpointRequest.to()Â creates a matcher for null/**Â if the actuator endpoint, for which the EndpointRequestÂ has been created, is disabled or not exposed.
 	
Your application may be affected by this if all the following conditions are met:
 	
 * You use Spring Security
 * EndpointRequest.to()Â has been used in a Spring Security chain configuration
 * The endpoint which EndpointRequestÂ references is disabled or not exposed via web
 * Your application handles requests to /nullÂ and this path needs protection
 	
You are not affected if any of the following is true:
 	
 * You don't use Spring Security
 * You don't use EndpointRequest.to()
 * The endpoint which EndpointRequest.to()Â refers to is enabled and is exposed
 * Your application does not handle requests to /nullÂ or this path does not need protection
	CVE-2025-22235	High		sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/BOOT-INF/lib/spring-boot-3.4.2.jar;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.springframework.boot:spring-boot:3.4.2/org.springframework.boot:spring-boot:3.4.2;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.springframework.boot:spring-boot:3.4.2/org.springframework.boot:spring-boot:3.4.2
					org.springframework.boot:spring-boot	<= 2.7.24.2,3.1.0 <= Version <= 3.1.15.2,3.2.0 <= Version <= 3.2.13.2,3.3.0 <= Version <= 3.3.10,3.4.0 <= Version <= 3.4.4	3.3.11,3.4.5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability

Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u391, 8u391-perf, 11.0.21, 17.0.9, 21.0.1; Oracle GraalVM for JDK: 17.0.9, 21.0.1; Oracle GraalVM Enterprise Edition: 20.3.12, 21.3.8 and 22.3.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector:	CVE-2024-20918	High		sha256__6ce99fdf16e86bd02f6ad66a0e1334878528b5a4b5487850a76e0c08a7a27d56.tar.gz/usr/local/openjdk-17/lib/libjavajpeg.so;
				sha256__6ce99fdf16e86bd02f6ad66a0e1334878528b5a4b5487850a76e0c08a7a27d56.tar.gz/usr/local/openjdk-17/bin/javap;
				sha256__6ce99fdf16e86bd02f6ad66a0e1334878528b5a4b5487850a76e0c08a7a27d56.tar.gz/usr/local/openjdk-17/bin/java;
				sha256__6ce99fdf16e86bd02f6ad66a0e1334878528b5a4b5487850a76e0c08a7a27d56.tar.gz/usr/local/openjdk-17/bin/javac;
				sha256__6ce99fdf16e86bd02f6ad66a0e1334878528b5a4b5487850a76e0c08a7a27d56.tar.gz/usr/local/openjdk-17/bin/javadoc;
				sha256__6ce99fdf16e86bd02f6ad66a0e1334878528b5a4b5487850a76e0c08a7a27d56.tar.gz/usr/local/openjdk-17/lib/libjava.so
					oracle:openjdk	11.0 <= Version <= 11.0.21,17.0 <= Version <= 17.0.9,21.0 <= Version <= 21.0.1		0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
(CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).		🟥							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.	CVE-2023-0464	High			debian:bullseye:openssl	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable
A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.	CVE-2023-0464	High			debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A vulnerability found in gnutls. This security flaw happens because of a double free error occurs during verification of pkcs7 signatures in gnutls_pkcs7_verify function.	CVE-2022-2509	High			debian:bullseye:libgnutls30	< 3.7.1-5+deb11u2	3.7.1-5+deb11u2	0001-01-01T00:00:00Z	Not Applicable

			JFrog			Infected	Fix		
Summary	**CVEs**	**Severity**	**Severity**	**Component Physical Paths**	**Component**	**Version**	**Version**	**Edited**	**Applicability**
Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit. OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(n^2)	CVE-2023-2650	Medium	Medium		debian:bullseye:openssl	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
with 'n' being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL...		🟧	🟧						

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Processing some specially crafted ASN.1 object identifiers or data containing them may be very slow. Impact summary: Applications that use OBJ_obj2txt() directly, or use any of the OpenSSL subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS with no message size limit may experience notable to very long delays when processing those messages, which may lead to a Denial of Service. An OBJECT IDENTIFIER is composed of a series of numbers - sub-identifiers - most of which have no size limit. OBJ_obj2txt() may be used to translate an ASN.1 OBJECT IDENTIFIER given in DER encoding form (using the OpenSSL type ASN1_OBJECT) to its canonical numeric text form, which are the sub-identifiers of the OBJECT IDENTIFIER in decimal form, separated by periods. When one of the sub-identifiers in the OBJECT IDENTIFIER is very large (these are sizes that are seen as absurdly large, taking up tens or hundreds of KiBs), the translation to a decimal number in text may take a very long time. The time complexity is O(n^2)	CVE-2023-2650	Medium	Medium		debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
with 'n' being the size of the sub-identifiers in bytes (*). With OpenSSL 3.0, support to fetch cryptographic algorithms using names / identifiers in string form was introduced. This includes using OBJECT IDENTIFIERs in canonical numeric text form as identifiers for fetching algorithms. Such OBJECT IDENTIFIERs may be received through the ASN.1 structure AlgorithmIdentifier, which is commonly used in multiple protocols to specify what cryptographic algorithm should be used to sign or verify, encrypt or decrypt, or digest passed data. Applications that call OBJ_obj2txt() directly with untrusted data are affected, with any version of OpenSSL. If the use is for the mere purpose of display, the severity is considered low. In OpenSSL 3.0 and newer, this affects the subsystems OCSP, PKCS7/SMIME, CMS, CMP/CRMF or TS. It also impacts anything that processes X.509 certificates, including simple things like verifying its signature. The impact on TLS is relatively low, because all versions of OpenSSL...									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).	CVE-2022-2097	Medium	Medium		debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-01-08T19:26:00Z	Not Applicable
AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p).	CVE-2022-2097	Medium	Medium		debian:bullseye:openssl	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	2023-01-08T19:26:00Z	Not Applicable
A flaw was found in glibc. In an uncommon situation, the gaih_inet function may use memory that has been freed, resulting in an application crash. This issue is only exploitable when the getaddrinfo function is called and the hosts database in /etc/nsswitch.conf is configured with SUCCESS=continue or SUCCESS=merge.	CVE-2023-4813	Medium	Low		debian:bullseye:libc-bin	All Versions		0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in glibc. In an uncommon situation, the gaih_inet function may use memory that has been freed, resulting in an application crash. This issue is only exploitable when the getaddrinfo function is called and the hosts database in /etc/nsswitch.conf is configured with SUCCESS=continue or SUCCESS=merge.	CVE-2023-4813	Medium	Low		debian:bullseye:libc6	All Versions		0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification. As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument. Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.	CVE-2023-0466	Medium			debian:bullseye:openssl	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The function X509_VERIFY_PARAM_add0_policy() is documented to implicitly enable the certificate policy check when doing certificate verification. However the implementation of the function does not enable the check which allows certificates with invalid or incorrect policies to pass the certificate verification. As suddenly enabling the policy check could break existing deployments it was decided to keep the existing behavior of the X509_VERIFY_PARAM_add0_policy() function. Instead the applications that require OpenSSL to perform certificate policy check need to use X509_VERIFY_PARAM_set1_policies() or explicitly enable the policy check by calling X509_VERIFY_PARAM_set_flags() with the X509_V_FLAG_POLICY_CHECK flag argument. Certificate policy checks are disabled by default in OpenSSL and are not commonly used by applications.	CVE-2023-0466	Medium			debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.	CVE-2023-0465	Medium			debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Applications that use a non-default option when verifying certificates may be vulnerable to an attack from a malicious CA to circumvent certain checks. Invalid certificate policies in leaf certificates are silently ignored by OpenSSL and other certificate policy checks are skipped for that certificate. A malicious CA could use this to deliberately assert invalid certificate policies in order to circumvent policy checking on the certificate altogether. Policy processing is disabled by default but can be enabled by passing the `-policy' argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()' function.	CVE-2023-0465	Medium			debian:bullseye:openssl	< 1.1.1n-0+deb11u5	1.1.1n-0+deb11u5	0001-01-01T00:00:00Z	Not Applicable
It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.	CVE-2011-3374	Low	High		debian:bullseye:apt	All Versions		2023-01-08T19:25:00Z	Not Applicable
It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the master keyring, leading to a potential man-in-the-middle attack.	CVE-2011-3374	Low	High		debian:bullseye:libapt-pkg6.0	All Versions		2023-01-08T19:25:00Z	Not Applicable
libpcre in PCRE before 8.43 allows a subject buffer over-read in JIT when UTF is disabled, and \X or \R has more than one fixed quantifier, a related issue to CVE-2019-20454.	CVE-2019-20838	Low	Medium		debian:bullseye:libpcre3	All Versions		2023-01-08T19:31:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bullseye:libkrb5support0	All Versions		2023-01-08T19:26:00Z	Not Applicable
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bullseye:libkrb5-3	All Versions		2023-01-08T19:26:00Z	Not Applicable
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bullseye:libgssapi-krb5-2	All Versions		2023-01-08T19:26:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dbentry->n_key_data" in kadmin/dbutil/dump.c that can store 16-bit data but unknowingly the developer has assigned a "u4" variable to it, which is for 32-bit data. An attacker can use this vulnerability to affect other artifacts of the database as we know that a Kerberos database dump file contains trusted data.	CVE-2018-5709	Low	Low		debian:bullseye:libk5crypto3	All Versions		2023-01-08T19:26:00Z	Not Applicable
Integer overflow vulnerability in pcre2test before 10.41 allows attackers to cause a denial of service or other unspecified impacts via negative input.	CVE-2022-41409	Low	Low		debian:bullseye:libpcre2-8-0	All Versions		0001-01-01T00:00:00Z	Not Applicable
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bullseye:mount	All Versions		2023-01-08T19:26:00Z	Not Applicable
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bullseye:libsmartcols1	All Versions		2023-01-08T19:26:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bullseye:libmount1	All Versions		2023-01-08T19:26:00Z	Not Applicable
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bullseye:bsdutils	All Versions		2023-01-08T19:26:00Z	Not Applicable
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bullseye:libblkid1	All Versions		2023-01-08T19:26:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bullseye:util-linux	All Versions		2023-01-08T19:26:00Z	Not Applicable
A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	CVE-2022-0563	Low	Low		debian:bullseye:libuuid1	All Versions		2023-01-08T19:26:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is	CVE-2024-5535	Low			debian:bullseye:libssl1.1	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of ...		🟨							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Calling the OpenSSL API function SSL_select_next_proto with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application beahviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the SSL_select_next_proto function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function SSL_select_next_proto is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is	CVE-2024-5535	Low			debian:bullseye:openssl	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The SSL_select_next_proto function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where SSL_select_next_proto is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of ...									
Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 4) or possibly have unspecified other impact via a crafted file.	CVE-2017-7245	Low			debian:bullseye:libpcre3	All Versions		0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Stack-based buffer overflow in the pcre32_copy_substring function in pcre_get.c in libpcre1 in PCRE 8.40 allows remote attackers to cause a denial of service (WRITE of size 268) or possibly have unspecified other impact via a crafted file.	CVE-2017-7246	Low			debian:bullseye:libpcre3	All Versions		0001-01-01T00:00:00Z	Not Applicable
nscd: Stack-based buffer overflow in netgroup cache If the Name Service Cache Daemon's (nscd) fixed size cache is exhausted by client requests then a subsequent client request for netgroup data may result in a stack-based buffer overflow. This flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33599	Unknown	High		debian:bullseye:libc6	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Applicable
nscd: Stack-based buffer overflow in netgroup cache If the Name Service Cache Daemon's (nscd) fixed size cache is exhausted by client requests then a subsequent client request for netgroup data may result in a stack-based buffer overflow. This flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33599	Unknown	High		debian:bullseye:libc-bin	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Applicable
The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable.	CVE-2024-2961	Unknown	High		debian:bullseye:libc-bin	< 2.31-13+deb11u9	2.31-13+deb11u9	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The iconv() function in the GNU C Library versions 2.39 and older may overflow the output buffer passed to it by up to 4 bytes when converting strings to the ISO-2022-CN-EXT character set, which may be used to crash an application or overwrite a neighbouring variable.	CVE-2024-2961	Unknown	High		debian:bullseye:libc6	< 2.31-13+deb11u9	2.31-13+deb11u9	0001-01-01T00:00:00Z	Not Applicable
nscd: Null pointer crashes after notfound response If the Name Service Cache Daemon's (nscd) cache fails to add a not-found netgroup response to the cache, the client request can result in a null pointer dereference. This flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33600	Unknown	Medium		debian:bullseye:libc-bin	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Applicable
nscd: Null pointer crashes after notfound response If the Name Service Cache Daemon's (nscd) cache fails to add a not-found netgroup response to the cache, the client request can result in a null pointer dereference. This flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33600	Unknown	Medium		debian:bullseye:libc6	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer	CVE-2024-4741	Unknown			debian:bullseye:openssl	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer	CVE-2024-4741	Unknown			debian:bullseye:libssl1.1	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Applicable

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.									
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bullseye:libsystemd0	< 247.3-7+deb11u6	247.3-7+deb11u6	0001-01-01T00:00:00Z	Undetermined

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Certain DNSSEC aspects of the DNS protocol (in RFC 4033, 4034, 4035, 6840, and related RFCs) allow remote attackers to cause a denial of service (CPU consumption) via one or more DNSSEC responses, aka the "KeyTrap" issue. One of the concerns is that, when there is a zone with many DNSKEY and RRSIG records, the protocol specification implies that an algorithm must evaluate all combinations of DNSKEY and RRSIG records.	CVE-2023-50387	High	High		debian:bullseye:libudev1	< 247.3-7+deb11u6	247.3-7+deb11u6	0001-01-01T00:00:00Z	Undetermined
CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HTTPS.	CVE-2023-31484	High	High		debian:bullseye:perl-base	< 5.32.1-4+deb11u4	5.32.1-4+deb11u4	0001-01-01T00:00:00Z	Undetermined
A flaw was found in glibc. An off-by-one buffer overflow and underflow in getcwd() may lead to memory corruption when the size of the buffer is exactly 1. A local attacker who can control the input buffer and size passed to getcwd() in a setuid program could use this flaw to potentially execute arbitrary code and escalate their privileges on the system.	CVE-2021-3999	High	Medium		debian:bullseye:libc6	< 2.31-13+deb11u4	2.31-13+deb11u4	2023-01-08T19:25:00Z	Undetermined
A flaw was found in glibc. An off-by-one buffer overflow and underflow in getcwd() may lead to memory corruption when the size of the buffer is exactly 1. A local attacker who can control the input buffer and size passed to getcwd() in a setuid program could use this flaw to potentially execute arbitrary code and escalate their privileges on the system.	CVE-2021-3999	High	Medium		debian:bullseye:libc-bin	< 2.31-13+deb11u4	2.31-13+deb11u4	2023-01-08T19:25:00Z	Undetermined
A flaw was found in the bash package, where a heap-buffer overflow can occur in valid parameter_transform. This issue may lead to memory problems.	CVE-2022-3715	High	Low		debian:bullseye:bash	All Versions		2023-01-22T22:11:00Z	Undetermined

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.	CVE-2022-29458	High	Low		debian:bullseye:ncurses-base	< 6.2+20201114-2+deb11u1	6.2+20201114-2+deb11u1	2023-05-18T07:43:00Z	Undetermined
ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.	CVE-2022-29458	High	Low		debian:bullseye:ncurses-bin	< 6.2+20201114-2+deb11u1	6.2+20201114-2+deb11u1	2023-05-18T07:43:00Z	Undetermined
ncurses 6.3 before patch 20220416 has an out-of-bounds read and segmentation violation in convert_strings in tinfo/read_entry.c in the terminfo library.	CVE-2022-29458	High	Low		debian:bullseye:libtinfo6	< 6.2+20201114-2+deb11u1	6.2+20201114-2+deb11u1	2023-05-18T07:43:00Z	Undetermined
An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.	CVE-2022-1304	High	Low		debian:bullseye:e2fsprogs	< 1.46.2-2+deb11u1	1.46.2-2+deb11u1	2023-01-08T19:26:00Z	Undetermined
An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.	CVE-2022-1304	High	Low		debian:bullseye:libcom-err2	< 1.46.2-2+deb11u1	1.46.2-2+deb11u1	2023-01-08T19:26:00Z	Undetermined
An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.	CVE-2022-1304	High	Low		debian:bullseye:libext2fs2	< 1.46.2-2+deb11u1	1.46.2-2+deb11u1	2023-01-08T19:26:00Z	Undetermined
An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.	CVE-2022-1304	High	Low		debian:bullseye:libss2	< 1.46.2-2+deb11u1	1.46.2-2+deb11u1	2023-01-08T19:26:00Z	Undetermined

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An out-of-bounds read/write vulnerability was found in e2fsprogs 1.46.5. This issue leads to a segmentation fault and possibly arbitrary code execution via a specially crafted filesystem.	CVE-2022-1304	High	Low		debian:bullseye:logsave	< 1.46.2-2+deb11u1	1.46.2-2+deb11u1	2023-01-08T19:26:00Z	Undetermined
In libtirpc before 1.3.3rc1, remote attackers could exhaust the file descriptors of a process that uses libtirpc because idle TCP connections are mishandled. This can, in turn, lead to an svc_run infinite loop without accepting new connections.	CVE-2021-46828	High			debian:bullseye:libtirpc-common	< 1.3.1-1+deb11u1	1.3.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
In libtirpc before 1.3.3rc1, remote attackers could exhaust the file descriptors of a process that uses libtirpc because idle TCP connections are mishandled. This can, in turn, lead to an svc_run infinite loop without accepting new connections.	CVE-2021-46828	High			debian:bullseye:libtirpc3	< 1.3.1-1+deb11u1	1.3.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service.	CVE-2022-3821	Medium	Low		debian:bullseye:libsystemd0	< 247.3-7+deb11u2	247.3-7+deb11u2	2022-12-31T17:43:00Z	Not Covered
An off-by-one Error issue was discovered in Systemd in format_timespan() function of time-util.c. An attacker could supply specific values for time and accuracy that leads to buffer overrun in format_timespan(), leading to a Denial of Service.	CVE-2022-3821	Medium	Low		debian:bullseye:libudev1	< 247.3-7+deb11u2	247.3-7+deb11u2	2022-12-31T17:43:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
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.	CVE-2025-3576	Medium			debian:bullseye:libk5crypto3	All Versions		0001-01-01T00:00:00Z	Not Covered
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.	CVE-2025-3576	Medium			debian:bullseye:libkrb5-3	All Versions		0001-01-01T00:00:00Z	Not Covered
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.	CVE-2025-3576	Medium			debian:bullseye:libgssapi-krb5-2	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
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.	CVE-2025-3576	Medium			debian:bullseye:libkrb5support0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant.	CVE-2024-0727	Medium			debian:bullseye:libssl1.1	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered
The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant.	CVE-2024-0727	Medium			debian:bullseye:openssl	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered
The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-22365	Medium			debian:bullseye:libpam-runtime	All Versions		0001-01-01T00:00:00Z	Not Covered
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-22365	Medium			debian:bullseye:libpam-modules-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-22365	Medium			debian:bullseye:libpam0g	All Versions		0001-01-01T00:00:00Z	Not Covered
linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked login process) via mkfifo because the openat call (for protect_dir) lacks O_DIRECTORY.	CVE-2024-22365	Medium			debian:bullseye:libpam-modules	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in systemd-resolved. This issue may allow systemd-resolved to accept records of DNSSEC-signed domains even when they have no signature, allowing man-in-the-middles (or the upstream DNS resolver) to manipulate records.	CVE-2023-7008	Medium			debian:bullseye:libsystemd0	< 247.3-7+deb11u6	247.3-7+deb11u6	0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in systemd-resolved. This issue may allow systemd-resolved to accept records of DNSSEC-signed domains even when they have no signature, allowing man-in-the-middles (or the upstream DNS resolver) to manipulate records.	CVE-2023-7008	Medium			debian:bullseye:libudev1	< 247.3-7+deb11u6	247.3-7+deb11u6	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bullseye:libtinfo6	All Versions		0001-01-01T00:00:00Z	Not Covered
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bullseye:ncurses-base	All Versions		0001-01-01T00:00:00Z	Not Covered
NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	CVE-2023-50495	Medium			debian:bullseye:ncurses-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found that the response times to malformed ciphertexts in RSA-PSK ClientKeyExchange differ from response times of ciphertexts with correct PKCS#1 v1.5 padding.	CVE-2023-5981	Medium			debian:bullseye:libgnutls30	< 3.7.1-5+deb11u4	3.7.1-5+deb11u4	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and	CVE-2023-5678	Medium			debian:bullseye:openssl	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.		🟧							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and	CVE-2023-5678	Medium			debian:bullseye:libssl1.1	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.		🟧							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in glibc. In an extremely rare situation, the getaddrinfo function may access memory that has been freed, resulting in an application crash. This issue is only exploitable when a NSS module implements only the _nss_*_gethostbyname2_r and _nss_*_getcanonname_r hooks without implementing the _nss_*_gethostbyname3_r hook. The resolved name should return a large number of IPv6 and IPv4, and the call to the getaddrinfo function should have the AF_INET6 address family with AI_CANONNAME, AI_ALL and AI_V4MAPPED as flags.	CVE-2023-4806	Medium			debian:bullseye:libc-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in glibc. In an extremely rare situation, the getaddrinfo function may access memory that has been freed, resulting in an application crash. This issue is only exploitable when a NSS module implements only the _nss_*_gethostbyname2_r and _nss_*_getcanonname_r hooks without implementing the _nss_*_gethostbyname3_r hook. The resolved name should return a large number of IPv6 and IPv4, and the call to the getaddrinfo function should have the AF_INET6 address family with AI_CANONNAME, AI_ALL and AI_V4MAPPED as flags.	CVE-2023-4806	Medium			debian:bullseye:libc6	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.	CVE-2023-4641	Medium			debian:bullseye:passwd	< 1:4.8.1-1+deb11u1	1:4.8.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the password twice. If the password fails on the second attempt, shadow-utils fails in cleaning the buffer used to store the first entry. This may allow an attacker with enough access to retrieve the password from the memory.	CVE-2023-4641	Medium			debian:bullseye:login	< 1:4.8.1-1+deb11u1	1:4.8.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count.	CVE-2023-36054	Medium			debian:bullseye:libkrb5-3	< 1.18.3-6+deb11u4	1.18.3-6+deb11u4	0001-01-01T00:00:00Z	Not Covered
lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count.	CVE-2023-36054	Medium			debian:bullseye:libk5crypto3	< 1.18.3-6+deb11u4	1.18.3-6+deb11u4	0001-01-01T00:00:00Z	Not Covered
lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count.	CVE-2023-36054	Medium			debian:bullseye:libkrb5support0	< 1.18.3-6+deb11u4	1.18.3-6+deb11u4	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
lib/kadm5/kadm_rpc_xdr.c in MIT Kerberos 5 (aka krb5) before 1.20.2 and 1.21.x before 1.21.1 frees an uninitialized pointer. A remote authenticated user can trigger a kadmind crash. This occurs because _xdr_kadm5_principal_ent_rec does not validate the relationship between n_key_data and the key_data array count.	CVE-2023-36054	Medium			debian:bullseye:libgssapi-krb5-2	< 1.18.3-6+deb11u4	1.18.3-6+deb11u4	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions.	CVE-2023-3817	Medium			debian:bullseye:openssl	< 1.1.1v-0~deb11u1	1.1.1v-0~deb11u1	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.									

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions.	CVE-2023-3817	Medium			debian:bullseye:libssl1.1	< 1.1.1v-0~deb11u1	1.1.1v-0~deb11u1	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.		🟧							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be	CVE-2023-3446	Medium			debian:bullseye:libssl1.1	< 1.1.1v-0~deb11u1	1.1.1v-0~deb11u1	0001-01-01T00:00:00Z	Not Covered

			JFrog			Infected	Fix		
Summary	**CVEs**	**Severity**	**Severity**	**Component Physical Paths**	**Component**	**Version**	**Version**	**Edited**	**Applicability**
vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.		🟧							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be	CVE-2023-3446	Medium			debian:bullseye:openssl	< 1.1.1v-0~deb11u1	1.1.1v-0~deb11u1	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.		🟧							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.	CVE-2022-4304	Medium			debian:bullseye:openssl	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A timing based side channel exists in the OpenSSL RSA Decryption implementation which could be sufficient to recover a plaintext across a network in a Bleichenbacher style attack. To achieve a successful decryption an attacker would have to be able to send a very large number of trial messages for decryption. The vulnerability affects all RSA padding modes: PKCS#1 v1.5, RSA-OEAP and RSASVE. For example, in a TLS connection, RSA is commonly used by a client to send an encrypted pre-master secret to the server. An attacker that had observed a genuine connection between a client and a server could use this flaw to send trial messages to the server and record the time taken to process them. After a sufficiently large number of messages the attacker could recover the pre-master secret used for the original connection and thus be able to decrypt the application data sent over that connection.	CVE-2022-4304	Medium			debian:bullseye:libssl1.1	< 1.1.1n-0+deb11u4	1.1.1n-0+deb11u4	0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in systemd. This security flaw can cause a local information leak due to systemd-coredump not respecting the fs.suid_dumpable kernel setting.	CVE-2022-4415	Medium			debian:bullseye:libsystemd0	< 247.3-7+deb11u2	247.3-7+deb11u2	0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in systemd. This security flaw can cause a local information leak due to systemd-coredump not respecting the fs.suid_dumpable kernel setting.	CVE-2022-4415	Medium			debian:bullseye:libudev1	< 247.3-7+deb11u2	247.3-7+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring and other constraints (e.g., use of GPGME) are met, allows signature forgery via injection into the status line.	CVE-2022-34903	Medium			debian:bullseye:gpgv	< 2.2.27-2+deb11u2	2.2.27-2+deb11u2	0001-01-01T00:00:00Z	Not Covered
A NULL pointer dereference flaw was found in GnuTLS. As Nettle's hash update functions internally call memcpy, providing zero-length input may cause undefined behavior. This flaw leads to a denial of service after authentication in rare circumstances.	CVE-2021-4209	Medium			debian:bullseye:libgnutls30	< 3.7.1-5+deb11u1	3.7.1-5+deb11u1	0001-01-01T00:00:00Z	Not Covered
HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN, has an insecure default TLS configuration where users must opt in to verify certificates.	CVE-2023-31486	Low	High		debian:bullseye:perl-base	All Versions		0001-01-01T00:00:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.	CVE-2018-20796	Low	Medium		debian:bullseye:libc-bin	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(\227|)(\\1\\1|t1|\\\2537)+' in grep.	CVE-2018-20796	Low	Medium		debian:bullseye:libc6	All Versions		2023-01-08T19:31:00Z	Not Covered
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern	CVE-2019-9192	Low	Medium		debian:bullseye:libc6	All Versions		2023-01-08T19:31:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '(|)(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern	CVE-2019-9192	Low	Medium		debian:bullseye:libc-bin	All Versions		2023-01-08T19:31:00Z	Not Covered
The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.	CVE-2010-4756	Low	Medium		debian:bullseye:libc-bin	All Versions		2023-01-08T19:30:00Z	Not Covered
The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in STAT commands to an FTP daemon, a different vulnerability than CVE-2010-2632.	CVE-2010-4756	Low	Medium		debian:bullseye:libc6	All Versions		2023-01-08T19:30:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bullseye:libsystemd0	All Versions		2023-01-08T19:25:00Z	Not Covered
systemd, when updating file permissions, allows local users to change the permissions and SELinux security contexts for arbitrary files via a symlink attack on unspecified files.	CVE-2013-4392	Low	Medium		debian:bullseye:libudev1	All Versions		2023-01-08T19:25:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server.	CVE-2020-13529	Low	Medium		debian:bullseye:libudev1	All Versions		2023-01-08T19:25:00Z	Not Covered
An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server.	CVE-2020-13529	Low	Medium		debian:bullseye:libsystemd0	All Versions		2023-01-08T19:25:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010022	Low	Low		debian:bullseye:libc6	All Versions		2023-01-08T19:25:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack guard protection. The component is: nptl. The attack vector is: Exploit stack buffer overflow vulnerability and use this bypass vulnerability to bypass stack guard. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010022	Low	Low		debian:bullseye:libc-bin	All Versions		2023-01-08T19:25:00Z	Not Covered
Tar 1.15.1 does not properly warn the user when extracting setuid or setgid files, which may allow local users or remote attackers to gain privileges.	CVE-2005-2541	Low	Low		debian:bullseye:tar	All Versions		2023-01-08T19:25:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability.	CVE-2019-1010025	Low			debian:bullseye:libc6	All Versions		0001-01-01T00:00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the heap addresses of pthread_created thread. The component is: glibc. NOTE: the vendor's position is "ASLR bypass itself is not a vulnerability.	CVE-2019-1010025	Low			debian:bullseye:libc-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010023	Low			debian:bullseye:libc-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. The impact is: In worst case attacker may evaluate privileges. The component is: libld. The attack vector is: Attacker sends 2 ELF files to victim and asks to run ldd on it. ldd execute code. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010023	Low			debian:bullseye:libc6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010024	Low			debian:bullseye:libc-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR using cache of thread stack and heap. The component is: glibc. NOTE: Upstream comments indicate "this is being treated as a non-security bug and no real threat.	CVE-2019-1010024	Low			debian:bullseye:libc6	All Versions		0001-01-01T00:00:00Z	Not Covered

Improper Handling of Case Sensitivity vulnerability in Apache Tomcat's GCI servlet allows security constraint bypass of security constraints that apply to the pathInfo component of a URI mapped to the CGI servlet.
 	
This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.6, from 10.1.0-M1 through 10.1.40, from 9.0.0.M1 through 9.0.104.
 	
Users are recommended to upgrade to version 11.0.7, 10.1.41 or 9.0.105, which fixes the issue.
	CVE-2025-46701	Low		sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/BOOT-INF/lib/tomcat-embed-core-10.1.34.jar;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/spring-petclinic-3.4.0-SNAPSHOT.jar/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34;
				sha256__e4ff3aae9ce49045db764b3a0f6726c96355b1169a38c48c9488266c146585c6.tar.gz/usr/local/spring-petclinic/META-INF/sbom/application.cdx.json/org.springframework.samples:spring-petclinic:3.4.0-SNAPSHOT/gav:/org.apache.tomcat.embed:tomcat-embed-core:10.1.34/org.apache.tomcat.embed:tomcat-embed-core:10.1.34
					org.apache.tomcat.embed:tomcat-embed-core	10.1.0-M1 <= Version < 10.1.41,11.0.0-M1 <= Version < 11.0.7,9.0.0.M1 <= Version < 9.0.105	10.1.41,11.0.7,9.0.105	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in GNU Coreutils. The sort utility's begfield() function is vulnerable to a heap buffer under-read. The program may access memory outside the allocated buffer if a user runs a crafted command using the traditional key format. A malicious input could lead to a crash or leak sensitive data.	CVE-2025-5278	Low			debian:bullseye:coreutils	All Versions		0001-01-01T00:00:00Z	Not Covered
cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improperly encodes plaintexts, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for Libgcrypt's ElGamal implementation.	CVE-2018-6829	Low			debian:bullseye:libgcrypt20	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only "named curves" are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an "exotic" curve encoding. The affected APIs include: EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions. Applications working with "exotic"	CVE-2024-9143	Low			debian:bullseye:libssl1.1	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.		🟨							

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only "named curves" are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an "exotic" curve encoding. The affected APIs include: EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions. Applications working with "exotic"	CVE-2024-9143	Low			debian:bullseye:openssl	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.									
In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replacement of a plain file with a symlink during use of the POSIX "-R -L" options, which allows local users to modify the ownership of arbitrary files by leveraging a race condition.	CVE-2017-18018	Low			debian:bullseye:coreutils	All Versions		0001-01-01T00:00:00Z	Not Covered
In PCRE 8.41, after compiling, a pcretest load test PoC produces a crash overflow in the function match() in pcre_exec.c because of a self-recursive call. NOTE: third parties dispute the relevance of this report, noting that there are options that can be used to limit the amount of stack that is used	CVE-2017-16231	Low			debian:bullseye:libpcre3	All Versions		0001-01-01T00:00:00Z	Not Covered
A timing-based side-channel flaw was found in libgcrypt's RSA implementation. This issue may allow a remote attacker to initiate a Bleichenbacher-style attack, which can lead to the decryption of RSA ciphertexts.	CVE-2024-2236	Low			debian:bullseye:libgcrypt20	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Low			debian:bullseye:libkrb5support0	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Low			debian:bullseye:libkrb5-3	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Low			debian:bullseye:libk5crypto3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	CVE-2024-26461	Low			debian:bullseye:libgssapi-krb5-2	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Low			debian:bullseye:libkrb5-3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Low			debian:bullseye:libkrb5support0	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Low			debian:bullseye:libk5crypto3	All Versions		0001-01-01T00:00:00Z	Not Covered
Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.	CVE-2024-26458	Low			debian:bullseye:libgssapi-krb5-2	All Versions		0001-01-01T00:00:00Z	Not Covered
In PCRE 8.41, the OP_KETRMAX feature in the match function in pcre_exec.c allows stack exhaustion (uncontrolled recursion) when processing a crafted regular expression.	CVE-2017-11164	Low			debian:bullseye:libpcre3	All Versions		0001-01-01T00:00:00Z	Undetermined

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Low			debian:bullseye:gcc-10-base	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Low			debian:bullseye:libstdc++6	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Low			debian:bullseye:gcc-9-base	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
DISPUTEDA failure in the -fstack-protector feature in GCC-based toolchains that target AArch64 allows an attacker to exploit an existing buffer overflow in dynamically-sized local variables in your application without this being detected. This stack-protector failure only applies to C99-style dynamically-sized local variables or those created using alloca(). The stack-protector operates as intended for statically-sized local variables. The default behavior when the stack-protector detects an overflow is to terminate your application, resulting in controlled loss of availability. An attacker who can exploit a buffer overflow without triggering the stack-protector might be able to change program flow control to cause an uncontrolled loss of availability or to go further and affect confidentiality or integrity. NOTE: The GCC project argues that this is a missed hardening bug and not a vulnerability by itself.	CVE-2023-4039	Low			debian:bullseye:libgcc-s1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bullseye:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, in some views, not all existing and sealed log messages are displayed. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31437	Low			debian:bullseye:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bullseye:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can modify the contents of past events in a sealed log file and then adjust the file such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31439	Low			debian:bullseye:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bullseye:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered
An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then resume log sealing such that checking the integrity shows no error, despite modifications. NOTE: the vendor reportedly sent "a reply denying that any of the finding was a security vulnerability."	CVE-2023-31438	Low			debian:bullseye:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In Shadow 4.13, it is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. Use of \r manipulations and Unicode characters to work around blocking of the : character make it possible to give the impression that a new user has been added. In other words, an adversary may be able to convince a system administrator to take the system offline (an indirect, social-engineered denial of service) by demonstrating that "cat /etc/passwd" shows a rogue user account.	CVE-2023-29383	Low			debian:bullseye:login	< 1:4.8.1-1+deb11u1	1:4.8.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
In Shadow 4.13, it is possible to inject control characters into fields provided to the SUID program chfn (change finger). Although it is not possible to exploit this directly (e.g., adding a new user fails because \n is in the block list), it is possible to misrepresent the /etc/passwd file when viewed. Use of \r manipulations and Unicode characters to work around blocking of the : character make it possible to give the impression that a new user has been added. In other words, an adversary may be able to convince a system administrator to take the system offline (an indirect, social-engineered denial of service) by demonstrating that "cat /etc/passwd" shows a rogue user account.	CVE-2023-29383	Low			debian:bullseye:passwd	< 1:4.8.1-1+deb11u1	1:4.8.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
GnuPG can be made to spin on a relatively small input by (for example) crafting a public key with thousands of signatures attached, compressed down to just a few KB.	CVE-2022-3219	Low			debian:bullseye:gpgv	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.	CVE-2011-3389	Low			debian:bullseye:libgnutls30	All Versions		0001-01-01T00:00:00Z	Not Covered
GNU Tar through 1.34 has a one-byte out-of-bounds read that results in use of uninitialized memory for a conditional jump. Exploitation to change the flow of control has not been demonstrated. The issue occurs in from_header in list.c via a V7 archive in which mtime has approximately 11 whitespace characters.	CVE-2022-48303	Low			debian:bullseye:tar	< 1.34+dfsg-1+deb11u1	1.34+dfsg-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows local users to obtain sensitive information regarding authentication attempts. NOTE: because sshd detects the insecure permissions and does not log certain events, this also prevents sshd from logging failed authentication attempts by remote attackers.	CVE-2007-5686	Low			debian:bullseye:passwd	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows local users to obtain sensitive information regarding authentication attempts. NOTE: because sshd detects the insecure permissions and does not log certain events, this also prevents sshd from logging failed authentication attempts by remote attackers.	CVE-2007-5686	Low			debian:bullseye:login	All Versions		0001-01-01T00:00:00Z	Not Covered
_is_safe in the File::Temp module for Perl does not properly handle symlinks.	CVE-2011-4116	Low			debian:bullseye:perl-base	All Versions		0001-01-01T00:00:00Z	Not Covered
shadow: TOCTOU (time-of-check time-of-use) race condition when copying and removing directory trees	CVE-2013-4235	Low			debian:bullseye:passwd	All Versions		0001-01-01T00:00:00Z	Not Covered
shadow: TOCTOU (time-of-check time-of-use) race condition when copying and removing directory trees	CVE-2013-4235	Low			debian:bullseye:login	All Versions		0001-01-01T00:00:00Z	Not Covered
chroot in GNU coreutils, when used with --userspec, allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.	CVE-2016-2781	Low			debian:bullseye:coreutils	All Versions		0001-01-01T00:00:00Z	Not Covered
The CIL compiler in SELinux 3.2 has a heap-based buffer over-read in ebitmap_match_any (called indirectly from cil_check_neverallow). This occurs because there is sometimes a lack of checks for invalid statements in an optional block.	CVE-2021-36087	Low			debian:bullseye:libsepol1	< 3.1-1+deb11u1	3.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
The CIL compiler in SELinux 3.2 has a use-after-free in cil_reset_classpermission (called from cil_reset_classperms_set and cil_reset_classperms_list).	CVE-2021-36086	Low			debian:bullseye:libsepol1	< 3.1-1+deb11u1	3.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __verify_map_perm_classperms and hashtab_map).	CVE-2021-36085	Low			debian:bullseye:libsepol1	< 3.1-1+deb11u1	3.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __cil_verify_classpermission and __cil_pre_verify_helper).	CVE-2021-36084	Low			debian:bullseye:libsepol1	< 3.1-1+deb11u1	3.1-1+deb11u1	0001-01-01T00:00:00Z	Not Covered
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bullseye:libsystemd0	< 247.3-7+deb11u6	247.3-7+deb11u6	0001-01-01T00:00:00Z	Undetermined
The Closest Encloser Proof aspect of the DNS protocol (in RFC 5155 when RFC 9276 guidance is skipped) allows remote attackers to cause a denial of service (CPU consumption for SHA-1 computations) via DNSSEC responses in a random subdomain attack, aka the "NSEC3" issue. The RFC 5155 specification implies that an algorithm must perform thousands of iterations of a hash function in certain situations.	CVE-2023-50868	Unknown	High		debian:bullseye:libudev1	< 247.3-7+deb11u6	247.3-7+deb11u6	0001-01-01T00:00:00Z	Undetermined
wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover.	CVE-2024-28085	Unknown	Low		debian:bullseye:util-linux	< 2.36.1-8+deb11u2	2.36.1-8+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover.	CVE-2024-28085	Unknown	Low		debian:bullseye:libsmartcols1	< 2.36.1-8+deb11u2	2.36.1-8+deb11u2	0001-01-01T00:00:00Z	Not Covered
wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover.	CVE-2024-28085	Unknown	Low		debian:bullseye:libuuid1	< 2.36.1-8+deb11u2	2.36.1-8+deb11u2	0001-01-01T00:00:00Z	Not Covered
wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover.	CVE-2024-28085	Unknown	Low		debian:bullseye:bsdutils	< 2.36.1-8+deb11u2	2.36.1-8+deb11u2	0001-01-01T00:00:00Z	Not Covered
wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover.	CVE-2024-28085	Unknown	Low		debian:bullseye:mount	< 2.36.1-8+deb11u2	2.36.1-8+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover.	CVE-2024-28085	Unknown	Low		debian:bullseye:libblkid1	< 2.36.1-8+deb11u2	2.36.1-8+deb11u2	0001-01-01T00:00:00Z	Not Covered
wall in util-linux through 2.40, often installed with setgid tty permissions, allows escape sequences to be sent to other users' terminals through argv. (Specifically, escape sequences received from stdin are blocked, but escape sequences received from argv are not blocked.) There may be plausible scenarios where this leads to account takeover.	CVE-2024-28085	Unknown	Low		debian:bullseye:libmount1	< 2.36.1-8+deb11u2	2.36.1-8+deb11u2	0001-01-01T00:00:00Z	Not Covered
CVE-2025-4598	CVE-2025-4598	Unknown			debian:bullseye:libsystemd0	All Versions		0001-01-01T00:00:00Z	Not Covered
CVE-2025-4598	CVE-2025-4598	Unknown			debian:bullseye:libudev1	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Perl threads have a working directory race condition where file operations may target unintended paths. If a directory handle is open at thread creation, the process-wide current working directory is temporarily changed in order to cloneÂ that handle for the new thread, which is visible from any third (orÂ more) thread already running. This may lead to unintended operationsÂ such as loading code or accessing files from unexpected locations,Â which a local attacker may be able to exploit. The bug was introduced in commitÂ 11a11ecf4bea72b17d250cfb43c897be1341861e and released in Perl version 5.13.6	CVE-2025-40909	Unknown			debian:bullseye:perl-base	All Versions		0001-01-01T00:00:00Z	Not Covered
Untrusted LD_LIBRARY_PATH environment variable vulnerability in the GNU C Library version 2.27 to 2.38 allows attacker controlled loading of dynamically shared library in statically compiled setuid binaries that call dlopen (including internal dlopen calls after setlocale or calls to NSS functions such as getaddrinfo).	CVE-2025-4802	Unknown			debian:bullseye:libc-bin	< 2.31-13+deb11u13	2.31-13+deb11u13	0001-01-01T00:00:00Z	Not Covered
Untrusted LD_LIBRARY_PATH environment variable vulnerability in the GNU C Library version 2.27 to 2.38 allows attacker controlled loading of dynamically shared library in statically compiled setuid binaries that call dlopen (including internal dlopen calls after setlocale or calls to NSS functions such as getaddrinfo).	CVE-2025-4802	Unknown			debian:bullseye:libc6	< 2.31-13+deb11u13	2.31-13+deb11u13	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
In GnuPG before 2.5.5, if a user chooses to import a certificate with certain crafted subkey data that lacks a valid backsig or that has incorrect usage flags, the user loses the ability to verify signatures made from certain other signing keys, aka a "verification DoS."	CVE-2025-30258	Unknown			debian:bullseye:gpgv	All Versions		0001-01-01T00:00:00Z	Not Covered
A flaw was found in GnuTLS, which relies on libtasn1 for ASN.1 data processing. Due to an inefficient algorithm in libtasn1, decoding certain DER-encoded certificate data can take excessive time, leading to increased resource consumption. This flaw allows a remote attacker to send a specially crafted certificate, causing GnuTLS to become unresponsive or slow, resulting in a denial-of-service condition.	CVE-2024-12243	Unknown			debian:bullseye:libgnutls30	< 3.7.1-5+deb11u7	3.7.1-5+deb11u7	0001-01-01T00:00:00Z	Not Covered
A flaw in libtasn1 causes inefficient handling of specific certificate data. When processing a large number of elements in a certificate, libtasn1 takes much longer than expected, which can slow down or even crash the system. This flaw allows an attacker to send a specially crafted certificate, causing a denial of service attack.	CVE-2024-12133	Unknown			debian:bullseye:libtasn1-6	< 4.16.0-2+deb11u2	4.16.0-2+deb11u2	0001-01-01T00:00:00Z	Not Covered
CVE-2025-24528	CVE-2025-24528	Unknown			debian:bullseye:libgssapi-krb5-2	< 1.18.3-6+deb11u6	1.18.3-6+deb11u6	0001-01-01T00:00:00Z	Not Covered
CVE-2025-24528	CVE-2025-24528	Unknown			debian:bullseye:libk5crypto3	< 1.18.3-6+deb11u6	1.18.3-6+deb11u6	0001-01-01T00:00:00Z	Not Covered
CVE-2025-24528	CVE-2025-24528	Unknown			debian:bullseye:libkrb5-3	< 1.18.3-6+deb11u6	1.18.3-6+deb11u6	0001-01-01T00:00:00Z	Not Covered
CVE-2025-24528	CVE-2025-24528	Unknown			debian:bullseye:libkrb5support0	< 1.18.3-6+deb11u6	1.18.3-6+deb11u6	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
When the assert() function in the GNU C Library versions 2.13 to 2.40 fails, it does not allocate enough space for the assertion failure message string and size information, which may lead to a buffer overflow if the message string size aligns to page size.	CVE-2025-0395	Unknown			debian:bullseye:libc-bin	< 2.31-13+deb11u12	2.31-13+deb11u12	0001-01-01T00:00:00Z	Not Covered
When the assert() function in the GNU C Library versions 2.13 to 2.40 fails, it does not allocate enough space for the assertion failure message string and size information, which may lead to a buffer overflow if the message string size aligns to page size.	CVE-2025-0395	Unknown			debian:bullseye:libc6	< 2.31-13+deb11u12	2.31-13+deb11u12	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation. Impact summary: A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low. The FIPS modules in 3.4, 3.3, 3.2, 3.1 and 3.0 are affected by this issue.	CVE-2024-13176	Unknown			debian:bullseye:openssl	< 1.1.1w-0+deb11u3	1.1.1w-0+deb11u3	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation. Impact summary: A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low. The FIPS modules in 3.4, 3.3, 3.2, 3.1 and 3.0 are affected by this issue.	CVE-2024-13176	Unknown			debian:bullseye:libssl1.1	< 1.1.1w-0+deb11u3	1.1.1w-0+deb11u3	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
shadow-utils (aka shadow) 4.4 through 4.17.0 establishes a default /etc/subuid behavior (e.g., uid 100000 through 165535 for the first user account) that can realistically conflict with the uids of users defined on locally administered networks, potentially leading to account takeover, e.g., by leveraging newuidmap for access to an NFS home directory (or same-host resources in the case of remote logins by these local network users). NOTE: it may also be argued that system administrators should not have assigned uids, within local networks, that are within the range that can occur in /etc/subuid.	CVE-2024-56433	Unknown			debian:bullseye:passwd	All Versions		0001-01-01T00:00:00Z	Not Covered
shadow-utils (aka shadow) 4.4 through 4.17.0 establishes a default /etc/subuid behavior (e.g., uid 100000 through 165535 for the first user account) that can realistically conflict with the uids of users defined on locally administered networks, potentially leading to account takeover, e.g., by leveraging newuidmap for access to an NFS home directory (or same-host resources in the case of remote logins by these local network users). NOTE: it may also be argued that system administrators should not have assigned uids, within local networks, that are within the range that can occur in /etc/subuid.	CVE-2024-56433	Unknown			debian:bullseye:login	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A vulnerability was found in PAM. The secret information is stored in memory, where the attacker can trigger the victim program to execute by sending characters to its standard input (stdin). As this occurs, the attacker can train the branch predictor to execute an ROP chain speculatively. This flaw could result in leaked passwords, such as those found in /etc/shadow while performing authentications.	CVE-2024-10041	Unknown			debian:bullseye:libpam-modules-bin	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in PAM. The secret information is stored in memory, where the attacker can trigger the victim program to execute by sending characters to its standard input (stdin). As this occurs, the attacker can train the branch predictor to execute an ROP chain speculatively. This flaw could result in leaked passwords, such as those found in /etc/shadow while performing authentications.	CVE-2024-10041	Unknown			debian:bullseye:libpam-runtime	All Versions		0001-01-01T00:00:00Z	Not Covered
A vulnerability was found in PAM. The secret information is stored in memory, where the attacker can trigger the victim program to execute by sending characters to its standard input (stdin). As this occurs, the attacker can train the branch predictor to execute an ROP chain speculatively. This flaw could result in leaked passwords, such as those found in /etc/shadow while performing authentications.	CVE-2024-10041	Unknown			debian:bullseye:libpam-modules	All Versions		0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A vulnerability was found in PAM. The secret information is stored in memory, where the attacker can trigger the victim program to execute by sending characters to its standard input (stdin). As this occurs, the attacker can train the branch predictor to execute an ROP chain speculatively. This flaw could result in leaked passwords, such as those found in /etc/shadow while performing authentications.	CVE-2024-10041	Unknown			debian:bullseye:libpam0g	All Versions		0001-01-01T00:00:00Z	Not Covered
nscd: netgroup cache assumes NSS callback uses in-buffer strings The Name Service Cache Daemon's (nscd) netgroup cache can corrupt memory when the NSS callback does not store all strings in the provided buffer. The flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33602	Unknown			debian:bullseye:libc6	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Covered
nscd: netgroup cache assumes NSS callback uses in-buffer strings The Name Service Cache Daemon's (nscd) netgroup cache can corrupt memory when the NSS callback does not store all strings in the provided buffer. The flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33602	Unknown			debian:bullseye:libc-bin	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
nscd: netgroup cache may terminate daemon on memory allocation failure The Name Service Cache Daemon's (nscd) netgroup cache uses xmalloc or xrealloc and these functions may terminate the process due to a memory allocation failure resulting in a denial of service to the clients. The flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33601	Unknown			debian:bullseye:libc6	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Covered
nscd: netgroup cache may terminate daemon on memory allocation failure The Name Service Cache Daemon's (nscd) netgroup cache uses xmalloc or xrealloc and these functions may terminate the process due to a memory allocation failure resulting in a denial of service to the clients. The flaw was introduced in glibc 2.15 when the cache was added to nscd. This vulnerability is only present in the nscd binary.	CVE-2024-33601	Unknown			debian:bullseye:libc-bin	< 2.31-13+deb11u10	2.31-13+deb11u10	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.	CVE-2024-2511	Unknown			debian:bullseye:libssl1.1	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.	CVE-2024-2511	Unknown			debian:bullseye:openssl	< 1.1.1w-0+deb11u2	1.1.1w-0+deb11u2	0001-01-01T00:00:00Z	Not Covered

Summary	CVEs	Severity	JFrog Severity	Component Physical Paths	Component	Infected Version	Fix Version	Edited	Applicability
A flaw was found in GnuTLS. The Minerva attack is a cryptographic vulnerability that exploits deterministic behavior in systems like GnuTLS, leading to side-channel leaks. In specific scenarios, such as when using the GNUTLS_PRIVKEY_FLAG_REPRODUCIBLE flag, it can result in a noticeable step in nonce size from 513 to 512 bits, exposing a potential timing side-channel.	CVE-2024-28834	Unknown			debian:bullseye:libgnutls30	< 3.7.1-5+deb11u6	3.7.1-5+deb11u6	0001-01-01T00:00:00Z	Not Covered
A flaw has been discovered in GnuTLS where an application crash can be induced when attempting to verify a specially crafted .pem bundle using the "certtool --verify-chain" command.	CVE-2024-28835	Unknown			debian:bullseye:libgnutls30	< 3.7.1-5+deb11u6	3.7.1-5+deb11u6	0001-01-01T00:00:00Z	Not Covered
In GNU tar before 1.35, mishandled extension attributes in a PAX archive can lead to an application crash in xheader.c.	CVE-2023-39804	Unknown			debian:bullseye:tar	< 1.34+dfsg-1+deb11u1	1.34+dfsg-1+deb11u1	0001-01-01T00:00:00Z	Not Covered