Vulnerability reports (Assets View)

Details

Report prints the first 200 records for each type of assets

(Please refer appendix for details of CVEs)

Containers (Vulnerable Workloads (No Vulnerabilities): 0% (9 Workload(s)))

Name	Namespace	Applications	Policy Mode	Group	High/Medium	Vulnerabilities	Scanned at
kube-proxy-kvh2j	kube-system	TCP/10249 TCP/10256	Discover	kube-proxy.kube-system	10 / 10 / 0	CVE-2024-33599 CVE-2018-20796 CVE-2017-18018 CVE-2019-1010023 CVE-2023-5678 CVE-2024-33601 CVE-2024-33602 CVE-2019-9192 CVE-2023-47108 CVE-2024-2961 CVE-2016-2781 GHSA-c5pj-mqfh-rvc3 CVE-2023-6237 CVE-2023-6129 CVE-2019-1010022 CVE-2024-33600 CVE-2019-1010024 CVE-2020-36325 CVE-2019-1010025 CVE-2024-0727	Aug 28, 2024
storage-provisioner	kube-system		Discover	storage.kube-system	10 / 8 / 0	CVE-2023-44487 CVE-2021-33194 CVE-2022-32149 CVE-2021-38561 CVE-2023-48795 CVE-2022-41717 CVE-2021-31525 CVE-2022-29526 CVE-2022-21698 CVE-2022-27191 CVE-2021-43565 CVE-2023-39325 CVE-2022-41723 CVE-2020-29652 CVE-2023-3978 CVE-2023-45288 CVE-2024-24786 CVE-2022-27664	Aug 28, 2024
dh157-ubuntu	default		Discover	dh157.default	5 / 9 / 8	CVE-2022-3219 CVE-2023-45918 CVE-2023-29383 CVE-2017-11164 CVE-2023-26604 CVE-2016-2781 CVE-2023-50495 CVE-2016-20013 CVE-2024-2236 CVE-2023-7008	Aug 28, 2024

Name	Namespace	Applications	Policy Mode	Group	High/Medium	Vulnerabilities	Scanned at
ubuntu	default		Discover	ubuntu.default	5 / 9 / 8	CVE-2023-45918 CVE-2016-20013 CVE-2023-26604 CVE-2016-2781 CVE-2024-2236 CVE-2023-50495 CVE-2023-7008 CVE-2017-11164 CVE-2022-3219 CVE-2023-29383	Aug 28, 2024
coredns-7db6d8ff4d-8tkdq	kube-system	TCP/9153 UDP/53 TCP/53 HTTP	Discover	coredns.kube-system	3 / 6 / 0	CVE-2024-22189 CVE-2023-39325 GHSA-m425-mq94-257g CVE-2023-49295 CVE-2023-48795 CVE-2023-45288 CVE-2023-44487 CVE-2024-24786	Aug 28, 2024
etcd-minikube	kube-system	etcd	Discover	etcd.kube-system	0 / 8 / 0	CVE-2023-45288 CVE-2024-24786	Aug 28, 2024
kube-controller-manager-minikube	kube-system	TCP/10257	Discover	kube-controller-manager.kube-system	2 / 1 / 0	CVE-2023-47108 CVE-2024-28180 GHSA-c5pj-mqfh-rvc3	Aug 28, 2024
kube-apiserver-minikube	kube-system	TCP/8443	Discover	kube-apiserver.kube-system	1 / 1 / 0	CVE-2023-47108 CVE-2024-28180	Aug 28, 2024
kube-scheduler-minikube	kube-system	TCP/10259	Discover	kube-scheduler.kube-system	1 / 0 / 0	CVE-2023-47108	Aug 28, 2024

Hosts (Vulnerable Hosts (NoVulnerabilities): 0% (1 host(s)))

Name	OS	Kernel Version	CPUs	Memory	Containers	Policy Mode	High/Medium	Vulnerabilities	Scanned at
minikube	Ubuntu 22.04.4 LTS	6.5.0-kali3-amd64	8	13.6 GB	22	Discover	54 / 38 / 25	CVE-2023-6597 CVE-2022-27943 CVE-2024-2511 CVE-2024-1737 CVE-2024-4076 CVE-2024-37370 CVE-2024-0397 CVE-2024-26462 CVE-2024-33599 CVE-2024-26458 CVE-2023-50495 CVE-2023-45918 CVE-2024-5535 CVE-2016-20013 CVE-2024-34397 CVE-2023-29383 CVE-2024-7264 CVE-2024-2236 CVE-2024-4741 CVE-2023-7008 CVE-2016-1585 CVE-2024-1975 CVE-2024-26461 CVE-2017-11164 CVE-2024-4032 CVE-2024-0760 CVE-2024-33602 CVE-2022-4899 CVE-2024-6387 CVE-2023-27043 CVE-2024-33601 CVE-2024-33600 CVE-2024-37371 CVE-2024-4603 CVE-2022-40735 CVE-2016-2781 CVE-2024-0450 CVE-2022-3219	Aug 28, 2024

Platforms

Name	Version	Base OS	High/Medium	Vulnerabilities
			0	No vulnerabilities

Images (Vulnerable Images (No Vulnerabilities): NaN% (0 image(s)))

Name	High/Medium	Vulnerabilities

Appendix (CVE list)

Name	Description	Score	Packages	Published at

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr>
<td>CVE-2024-5535</td>
<td>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 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 server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with</td>
<td>V2: 9
V3: 9.1</td>
<td>openssl
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.17</td></tr>
</table>
openssl/libssl3
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.17</td></tr>
</table>
</td>
<td>Jul 12, 2024
10:15:16</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td></td><td>the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a "no overlap" response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available.</td><td></td><td></td><td></td></tr>
<tr><td>CVE-2024-4741</td><td>Use After Free with SSL_free_buffers</td><td>V2: 4
V3: 5.6</td><td>openssl
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.17</td></tr>
</table>
openssl/libssl3
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.17</td></tr>
</table></td><td>Jun 11, 2024
08:00:00</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-0397</td><td>A defect was discovered in the Python “ssl” module where there is a memory race condition with the ssl.SSLContext methods “cert_store_stats()” and “get_ca_certs()”. The race condition can be triggered if the methods are called at the same time as certificates are loaded into the SSLContext, such as during the TLS handshake with a certificate directory configured. This issue is fixed in CPython 3.10.14, 3.11.9, 3.12.3, and 3.13.0a5.</td><td><b>V2:</b> 7
<b>V3:</b> 7.4</td><td>python3.10
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.5</td></tr></table>
python3.10/libpython3.10-minimal
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.5</td></tr></table>
python3.10/libpython3.10-stdlib
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.5</td></tr></table>
...(4 packages)</td><td>Jul 2, 2024
09:44:41</td></tr>
<tr><td>CVE-2023-6597</td><td>An issue was found in the CPython `tempfile.TemporaryDirectory` class affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The tempfile.TemporaryDirectory class would dereference symlinks during cleanup of permissions-related errors. This means users which can run privileged programs are potentially able to modify permissions of files referenced by symlinks in some circumstances.</td><td><b>V2:</b> 7
<b>V3:</b> 7.8</td><td>python3.10
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.4</td></tr></table>
python3.10/libpython3.10-minimal
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.4</td></tr></table>
python3.10/libpython3.10-stdlib
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.4</td></tr></table>
...(4 packages)</td><td>Jun 10, 2024
02:15:24</td></tr>
</table>

Name	Description	Score	Packages	Published at
CVE-2024-4603	Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary: Applications that use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA 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 functions EVP_PKEY_param_check() or EVP_PKEY_public_check() perform various checks on DSA parameters. Some of those computations take a long time if the modulus (\`p\` parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls EVP_PKEY_param_check() or EVP_PKEY_public_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL pkey 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 affected by this issue.	**V2:** 4 **V3:** 5.3	openssl **Impacted Version** / **Fixed Version** 3.0.2-0ubuntu1.15 / 3.0.2-0ubuntu1.17 openssl/libssl3 **Impacted Version** / **Fixed Version** 3.0.2-0ubuntu1.15 / 3.0.2-0ubuntu1.17	Aug 13, 2024 12:35:05
CVE-2024-1975	If a server hosts a zone containing a "KEY" Resource Record, or a resolver DNSSEC-validates a "KEY" Resource Record from a DNSSEC-signed domain in cache, a client can exhaust resolver CPU resources by sending a stream of SIG(0) signed requests. This issue affects BIND 9 versions 9.0.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.9.3-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.49-S1, and 9.18.11-S1 through 9.18.27-S1.	**V2:** 7 **V3:** 7.5	bind9/bind9-dnsutils **Impacted Version** / **Fixed Version** 1:9.18.18-0ubuntu0.22.04.2 / 1:9.18.28-0ubuntu0.22.04.1 bind9/bind9-host **Impacted Version** / **Fixed Version** 1:9.18.18-0ubuntu0.22.04.2 / 1:9.18.28-0ubuntu0.22.04.1 bind9/bind9-libs **Impacted Version** / **Fixed Version** 1:9.18.18-0ubuntu0.22.04.2 / 1:9.18.28-0ubuntu0.22.04.1 ...(4 packages)	Aug 1, 2024 09:46:16

Name	Description	Score	Packages			Published at
				Impacted Version	Fixed Version	
CVE-2024-2236	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.	V2: 4 V3: 5.9	libgcrypt20	1.9.4-3ubuntu3	N/A	Apr 25, 2024 01:15:49
				1.8.5-5ubuntu1.1	N/A	
CVE-2024-33601	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.	V2: 7 V3: 7.5	glibc/libc-bin	2.35-0ubuntu3.7	2.35-0ubuntu3.8	Jul 22, 2024 02:15:03
			glibc/libc6	2.36-9+deb12u4	2.36-9+deb12u7	
				2.35-0ubuntu3.7	2.35-0ubuntu3.8	
CVE-2023-50495	NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _nc_wrap_entry().	V2: 4 V3: 6.5	ncurses/libncurses6	6.3-2ubuntu0.1	N/A	Jan 30, 2024 10:15:08
				6.2-0ubuntu2.1	N/A	
			ncurses/libncursesw6	6.2-0ubuntu2.1	N/A	
				6.3-2ubuntu0.1	N/A	
			ncurses/libtinfo6	6.2-0ubuntu2.1	N/A	
				6.3-2ubuntu0.1	N/A	
			...(5 packages)			
CVE-2021-31525	golang.org/x/net/http/httpguts vulnerable to Uncontrolled Recursion golang.org/x/net/http/httpguts in Go before 1.15.12 and 1.16.x before 1.16.4 allows remote attackers to cause a denial of service (panic) via a large header to ReadRequest or ReadResponse. Server, Transport, and Client can each be affected in some configurations.	V2: 2.6 V3: 5.9	go:golang.org/x/net	0.0.0-20201224014010-6772e930b67b	0.0.0-20210428140749-89ef3d95e781	May 24, 2022 03:03:29

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2023-26604</td><td>systemd before 247 does not adequately block local privilege escalation for some Sudo configurations, e.g., plausible sudoers files in which the "systemctl status" command may be executed. Specifically, systemd does not set LESSSECURE to 1, and thus other programs may be launched from the less program. This presents a substantial security risk when running systemctl from Sudo, because less executes as root when the terminal size is too small to show the complete systemctl output.</td><td>V2: 7
V3: 7.8</td><td>systemd/libsystemd0
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>245.4-4ubuntu3.23</td><td>N/A</td></tr></table>
systemd/libudev1
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>245.4-4ubuntu3.23</td><td>N/A</td></tr></table></td><td>Nov 6, 2023
11:09:41</td></tr>
<tr><td>CVE-2019-9192</td><td>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</td><td>V2: 5
V3: 7.5</td><td>glibc/libc6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.36-9+deb12u4</td><td>N/A</td></tr></table></td><td>Aug 4, 2024
06:15:34</td></tr>
<tr><td>CVE-2024-26458</td><td>Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src /lib/rpc/pmap_rmt.c.</td><td>V2: 4
V3: 5.9</td><td>krb5/libgssapi-krb5-2
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>N/A</td></tr></table>
krb5/libk5crypto3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>N/A</td></tr></table>
krb5/libkrb5-3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>N/A</td></tr></table>
...(4 packages)</td><td>May 14, 2024
11:09:00</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-0450</td><td>An issue was found in the CPython `zipfile` module affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The zipfile module is vulnerable to “quoted-overlap” zip-bombs which exploit the zip format to create a zip-bomb with a high compression ratio. The fixed versions of CPython makes the zipfile module reject zip archives which overlap entries in the archive.</td><td>V2: 4
V3: 6.2</td><td>python3.10
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.4</td></tr></table>
python3.10/libpython3.10-minimal
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.4</td></tr></table>
python3.10/libpython3.10-stdlib
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.4</td></tr></table>
...(4 packages)</td><td>Jun 10, 2024
02:15:24</td></tr>
<tr><td>CVE-2023-6237</td><td>Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary: Applications that use the function EVP_PKEY_public_check() to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function EVP_PKEY_public_check() is called on RSA public keys, a computation is done to confirm that the RSA modulus, n, is composite. For valid RSA keys, n is a product of two or more large primes and this computation completes quickly. However, if n is an overly large prime, then this computation would take a long time. An application that calls EVP_PKEY_public_check() and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function EVP_PKEY_public_check() is not called from other OpenSSL functions however it is called from the OpenSSL pkey command line application. For that reason that application is also vulnerable if used with the '-pubin' and '-check' options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.</td><td>V2: 4
V3: 5.9</td><td>openssl/libssl3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.0.11-1~deb12u2</td><td>3.0.13-1~deb12u1</td></tr></table></td><td>Jun 10, 2024
01:16:16</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2022-40735</td><td>The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably make certain calculations unnecessarily expensive, because the 1996 van Oorschot and Wiener paper found that "(appropriately) short exponents" can be used when there are adequate subgroup constraints, and these short exponents can lead to less expensive calculations than for long exponents. This issue is different from CVE-2002-20001 because it is based on an observation about exponent size, rather than an observation about numbers that are not public keys. The specific situations in which calculation expense would constitute a server-side vulnerability depend on the protocol (e.g., TLS, SSH, or IKE) and the DHE implementation details. In general, there might be an availability concern because of server-side resource consumption from DHE modular-exponentiation calculations. Finally, it is possible for an attacker to exploit this vulnerability and CVE-2002-20001 together.</td><td>V2: 7
V3: 7.5</td><td>openssl
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.16</td></tr></table>
openssl/libssl3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.16</td></tr></table></td><td>Apr 23, 2024
03:15:42</td></tr>
<tr><td>CVE-2020-29652</td><td>golang.org/x/crypto/ssh NULL Pointer Dereference vulnerability
A nil pointer dereference in the golang.org/x/crypto/ssh component through v0.0.0-20201203163018-be400aefbc4c for Go allows remote attackers to cause a denial of service against SSH servers. An attacker can craft an authentication request message for the `gssapi-with-mic` method which will cause NewServerConn to panic via a nil pointer dereference if ServerConfig.GSSAPIWithMICConfig is nil.</td><td>V2: 5
V3: 7.5</td><td>go:golang.org/x/crypto
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201002170205-7f63de1d35b0</td><td>0.0.0-20201216223049-8b5274cf687f</td></tr></table></td><td>May 24, 2022
06:01:25</td></tr>
<tr><td>CVE-2018-20796</td><td>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.</td><td>V2: 5
V3: 7.5</td><td>glibc/libc6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.36-9+deb12u4</td><td>N/A</td></tr></table></td><td>Nov 6, 2023
09:56:20</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2022-41717</td><td>golang.org/x/net/http2 vulnerable to possible excessive memory growth
An attacker can cause excessive memory growth in a Go server accepting HTTP/2 requests. HTTP/2 server connections contain a cache of HTTP header keys sent by the client. While the total number of entries in this cache is capped, an attacker sending very large keys can cause the server to allocate approximately 64 MiB per open connection.</td><td>V2: 4
V3: 5.3</td><td>go:golang.org/x/net<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201224014010-6772e930b67b</td><td>0.4.0</td></tr></table></td><td>Dec 8, 2022
04:30:19</td></tr>
<tr><td>CVE-2021-33194</td><td>golang.org/x/net/html Infinite Loop vulnerability
Go through 1.15.12 and 1.16.x through 1.16.4 has a golang.org/x/net/html infinite loop via crafted ParseFragment input.</td><td>V2: 5
V3: 7.5</td><td>go:golang.org/x/net<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201224014010-6772e930b67b</td><td>0.0.0-20210520170846-37e1c6afe023</td></tr></table></td><td>May 24, 2022
03:03:21</td></tr>
<tr><td>CVE-2024-7264</td><td>libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the *time fraction*, leading to a `strlen()` getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when [CURLINFO_CERTINFO](https://curl.se/libcurl/c/CURLINFO_CERTINFO.html) is used.</td><td>V2: 4
V3: 6.5</td><td>curl<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>7.81.0-1ubuntu1.16</td><td>7.81.0-1ubuntu1.17</td></tr></table>curl/libcurl4<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>7.81.0-1ubuntu1.16</td><td>7.81.0-1ubuntu1.17</td></tr></table></td><td>Aug 12, 2024
01:30:51</td></tr>
<tr><td>CVE-2024-33600</td><td>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.</td><td>V2: 4
V3: 5.3</td><td>glibc/libc-bin<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.35-0ubuntu3.7</td><td>2.35-0ubuntu3.8</td></tr></table>glibc/libc6<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.36-9+deb12u4</td><td>2.36-9+deb12u7</td></tr><tr><td>2.35-0ubuntu3.7</td><td>2.35-0ubuntu3.8</td></tr></table></td><td>Jul 22, 2024
02:15:03</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-4076</td><td>Client queries that trigger serving stale data and that also require lookups in local authoritative zone data may result in an assertion failure. This issue affects BIND 9 versions 9.16.13 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.11.33-S1 through 9.11.37-S1, 9.16.13-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.27-S1.</td><td><b>V2:</b> 7
<b>V3:</b> 7.5</td><td>bind9/bind9-dnsutils
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr></table>
bind9/bind9-host
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr></table>
bind9/bind9-libs
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr></table>
...(4 packages)</td><td>Aug 1, 2024
09:59:24</td></tr>
<tr><td>CVE-2023-45918</td><td>ncurses 6.4-20230610 has a NULL pointer dereference in tgetstr in tinfo/lib_termcap.c.</td><td><b>V2:</b> 1
<b>V3:</b> 3.3</td><td>ncurses/libncurses6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>6.2-0ubuntu2.1</td><td>N/A</td></tr><tr><td>6.3-2ubuntu0.1</td><td>N/A</td></tr></table>
ncurses/libncursesw6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>6.2-0ubuntu2.1</td><td>N/A</td></tr><tr><td>6.3-2ubuntu0.1</td><td>N/A</td></tr></table>
ncurses/libtinfo6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>6.3-2ubuntu0.1</td><td>N/A</td></tr><tr><td>6.2-0ubuntu2.1</td><td>N/A</td></tr></table>
...(5 packages)</td><td>Mar 15, 2024
07:15:08</td></tr>
<tr><td>CVE-2021-43565</td><td>x/crypto/ssh vulnerable to panic via malformed packets
The x/crypto/ssh package before 0.0.0-20211202192323-5770296d904e of golang.org/x/crypto allows an unauthenticated attacker to panic an SSH server. When using AES-GCM or ChaCha20Poly1305, consuming a malformed packet which contains an empty plaintext causes a panic.</td><td><b>V2:</b> 7
<b>V3:</b> 7.5</td><td>go:golang.org/x/crypto
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201002170205-7f63de1d35b0</td><td>0.0.0-20211202192323-5770296d904e</td></tr></table></td><td>Sep 6, 2022
08:01:52</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2023-49295</td><td>quic-go's path validation mechanism can be exploited to cause denial of service
An attacker can cause its peer to run out of memory sending a large number of PATH_CHALLENGE frames. The receiver is supposed to respond to each PATH_CHALLENGE frame with a PATH_RESPONSE frame. The attacker can prevent the receiver from sending out (the vast majority of) these PATH_RESPONSE frames by collapsing the peers congestion window (by selectively acknowledging received packets) and by manipulating the peer's RTT estimate.
I published a more detailed description of the attack and its mitigation in this blog post: https://seemann.io/posts/2023-12-18-exploiting-quics-path-validation/
There's no way to mitigate this attack, please update quic-go to a version that contains the fix.</td><td>V2: 4
V3: 6.4</td><td>go:github.com/quic-go/quic-go<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.37.4</td><td>0.40.1;0.39.4;0.38.2;0.37.7</td></tr></table></td><td>Jan 10, 2024
10:08:40</td></tr>
<tr><td>CVE-2022-4899</td><td>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.</td><td>V2: 7
V3: 7.5</td><td>libzstd/libzstd1<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.4.8+dfsg-3build1</td><td>N/A</td></tr></table></td><td>Nov 6, 2023
10:59:16</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-0727</td><td>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. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.</td><td><b>V2:</b> 4
<b>V3:</b> 5.5</td><td>openssl/libssl3
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>3.0.11-1~deb12u2</td><td>3.0.13-1~deb12u1</td></tr>
</table></td><td>May 1, 2024
02:15:13</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr>
<td>CVE-2023-44487</td>
<td>HTTP/2 Stream Cancellation Attack
HTTP/2 Rapid reset attack
The HTTP/2 protocol allows clients to indicate to the server that a previous stream should be canceled by sending a RST_STREAM frame. The protocol does not require the client and server to coordinate the cancellation in any way, the client may do it unilaterally. The client may also assume that the cancellation will take effect immediately when the server receives the RST_STREAM frame, before any other data from that TCP connection is processed.
Abuse of this feature is called a Rapid Reset attack because it relies on the ability for an endpoint to send a RST_STREAM frame immediately after sending a request frame, which makes the other endpoint start working and then rapidly resets the request. The request is canceled, but leaves the HTTP/2 connection open.
The HTTP/2 Rapid Reset attack built on this capability is simple: The client opens a large number of streams at once as in the standard HTTP/2 attack, but rather than waiting for a response to each request stream from the server or proxy, the client cancels each request immediately.
The ability to reset streams immediately allows each connection to have an indefinite number of requests in flight. By explicitly canceling the requests, the attacker never exceeds the limit on the number of concurrent open streams. The number of in-flight requests is no longer dependent on the round-trip time (RTT), but only on the available network bandwidth.
In a typical HTTP/2 server implementation, the server will still have to do significant amounts of work for canceled requests, such as allocating new stream data structures, parsing the query and doing header decompression, and mapping the URL to a resource. For reverse proxy implementations, the request may be proxied to the backend server before the RST_STREAM frame is processed. The client on the other hand paid almost no costs for sending the requests. This creates an exploitable cost asymmetry between the server and the client.</td>
<td>V2: 4
V3: 5.3</td>
<td>go:golang.org/x/net
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>0.0.0-20201224014010-6772e930b67b</td><td>0.17.0</td></tr>
<tr><td>0.14.0</td><td>0.17.0</td></tr>
</table>
go:google.golang.org/grpc
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.57.0</td><td>1.58.3;1.57.1;1.56.3</td></tr>
</table>
</td>
<td>Oct 10, 2023
05:28:24</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td></td><td>Multiple software artifacts implementing HTTP/2 are affected. This advisory was originally ingested from the `swift-nio-http2` repo advisory and their original conent follows.
swift-nio-http2 specific advisory
swift-nio-http2 is vulnerable to a denial-of-service vulnerability in which a malicious client can create and then reset a large number of HTTP/2 streams in a short period of time. This causes swift-nio-http2 to commit to a large amount of expensive work which it then throws away, including creating entirely new `Channel`s to serve the traffic. This can easily overwhelm an `EventLoop` and prevent it from making forward progress.
swift-nio-http2 1.28 contains a remediation for this issue that applies reset counter using a sliding window. This constrains the number of stream resets that may occur in a given window of time. Clients violating this limit will have their connections torn down. This allows clients to continue to cancel streams for legitimate reasons, while constraining malicious actors.</td><td></td><td></td><td></td></tr>
<tr><td>CVE-2022-32149</td><td>golang.org/x/text/language Denial of service via crafted Accept-Language header
The BCP 47 tag parser has quadratic time complexity due to inherent aspects of its design. Since the parser is, by design, exposed to untrusted user input, this can be leveraged to force a program to consume significant time parsing Accept-Language headers. The parser cannot be easily rewritten to fix this behavior for various reasons. Instead the solution implemented in this CL is to limit the total complexity of tags passed into ParseAcceptLanguage by limiting the number of dashes in the string to 1000. This should be more than enough for the majority of real world use cases, where the number of tags being sent is likely to be in the single digits.
Specific Go Packages Affected
golang.org/x/text/language</td><td>V2: 7
V3: 7.5</td><td>go:golang.org/x/text<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.3.5</td><td>0.3.8</td></tr></table></td><td>Oct 14, 2022
03:00:40</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2023-29383</td><td>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.</td><td><b>V2:</b> 1
<b>V3:</b> 3.3</td><td>shadow/login<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:4.8.1-2ubuntu2.2</td><td>N/A</td></tr><tr><td>1:4.8.1-1ubuntu5.20.04.5</td><td>N/A</td></tr></table>shadow/passwd<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:4.8.1-1ubuntu5.20.04.5</td><td>N/A</td></tr><tr><td>1:4.8.1-2ubuntu2.2</td><td>N/A</td></tr></table></td><td>Apr 24, 2023
02:05:30</td></tr>
<tr><td>CVE-2024-28180</td><td>Go JOSE vulnerable to Improper Handling of Highly Compressed Data (Data Amplification)
Impact
An attacker could send a JWE containing compressed data that used large amounts of memory and CPU when decompressed by Decrypt or DecryptMulti. Those functions now return an error if the decompressed data would exceed 250kB or 10x the compressed size (whichever is larger). Thanks to Enze Wang@Alioth and Jianjun Chen@Zhongguancun Lab (@zer0yu and @chenjj) for reporting.
Patches
The problem is fixed in the following packages and versions:
- github.com/go-jose/go-jose/v4 version 4.0.1
- github.com/go-jose/go-jose/v3 version 3.0.3
- gopkg.in/go-jose/go-jose.v2 version 2.6.3
The problem will not be fixed in the following package because the package is archived:
- gopkg.in/square/go-jose.v2</td><td><b>V2:</b> 4
<b>V3:</b> 4.3</td><td>go:gopkg.in/square/go-jose.v2<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.6.0</td><td>N/A</td></tr></table></td><td>Mar 7, 2024
05:54:44</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-24786</td><td>Golang protojson.Unmarshal function infinite loop when unmarshaling certain forms of invalid JSON
The protojson.Unmarshal function can enter an infinite loop when unmarshaling certain forms of invalid JSON. This condition can occur when unmarshaling into a message which contains a google.protobuf.Any value, or when the UnmarshalOptions.DiscardUnknown option is set.</td><td>V2: 4
V3: 5.9</td><td>go:google.golang.org/protobuf
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.25.0</td><td>1.33.0</td></tr>
<tr><td>1.31.0</td><td>1.33.0</td></tr>
</table></td><td>Mar 5, 2024
07:31:27</td></tr>
<tr><td>CVE-2019-1010024</td><td>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.</td><td>V2: 5
V3: 5.3</td><td>glibc/libc6
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>2.36-9+deb12u4</td><td>N/A</td></tr>
</table></td><td>Aug 4, 2024
11:15:25</td></tr>
<tr><td>CVE-2024-1737</td><td>Resolver caches and authoritative zone databases that hold significant numbers of RRs for the same hostname (of any RTYPE) can suffer from degraded performance as content is being added or updated, and also when handling client queries for this name. This issue affects BIND 9 versions 9.11.0 through 9.11.37, 9.16.0 through 9.16.50, 9.18.0 through 9.18.27, 9.19.0 through 9.19.24, 9.11.4-S1 through 9.11.37-S1, 9.16.8-S1 through 9.16.50-S1, and 9.18.11-S1 through 9.18.27-S1.</td><td>V2: 7
V3: 7.5</td><td>bind9/bind9-dnsutils
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr>
</table>
bind9/bind9-host
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr>
</table>
bind9/bind9-libs
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr>
</table>
...(4 packages)</td><td>Aug 1, 2024
09:46:11</td></tr>
<tr><td>CVE-2024-2961</td><td>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.</td><td>V2: 7
V3: 7.3</td><td>glibc/libc6
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>2.36-9+deb12u4</td><td>2.36-9+deb12u6</td></tr>
</table></td><td>Jul 22, 2024
02:15:03</td></tr>
<tr><td>CVE-2019-1010025</td><td>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.</td><td>V2: 5
V3: 5.3</td><td>glibc/libc6
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>2.36-9+deb12u4</td><td>N/A</td></tr>
</table></td><td>Aug 4, 2024
11:15:25</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-37370</td><td>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.</td><td>V2: 7
V3: 7.4</td><td>krb5/libgssapi-krb5-2
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>1.19.2-2ubuntu0.4</td></tr></table>
krb5/libk5crypto3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>1.19.2-2ubuntu0.4</td></tr></table>
krb5/libkrb5-3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>1.19.2-2ubuntu0.4</td></tr></table>
...(4 packages)</td><td>Jul 1, 2024
08:37:24</td></tr>
<tr><td>CVE-2024-33602</td><td>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.</td><td>V2: 7
V3: 8.6</td><td>glibc/libc-bin
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.35-0ubuntu3.7</td><td>2.35-0ubuntu3.8</td></tr></table>
glibc/libc6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.36-9+deb12u4</td><td>2.36-9+deb12u7</td></tr><tr><td>2.35-0ubuntu3.7</td><td>2.35-0ubuntu3.8</td></tr></table></td><td>Jul 22, 2024
02:15:03</td></tr>
<tr><td>CVE-2020-36325</td><td>An issue was discovered in Jansson through 2.13.1. Due to a parsing error in json_loads, there's an out-of-bounds read-access bug. NOTE: the vendor reports that this only occurs when a programmer fails to follow the API specification</td><td>V2: 5
V3: 7.5</td><td>jansson/libjansson4
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.14-2</td><td>N/A</td></tr></table></td><td>Aug 4, 2024
02:15:43</td></tr>
<tr><td>CVE-2024-33599</td><td>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.</td><td>V2: 7
V3: 7.6</td><td>glibc/libc-bin
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.35-0ubuntu3.7</td><td>2.35-0ubuntu3.8</td></tr></table>
glibc/libc6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.36-9+deb12u4</td><td>2.36-9+deb12u7</td></tr><tr><td>2.35-0ubuntu3.7</td><td>2.35-0ubuntu3.8</td></tr></table></td><td>Jul 22, 2024
02:15:03</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2023-3978</td><td>Improper rendering of text nodes in golang.org/x/net/html
Text nodes not in the HTML namespace are incorrectly literally rendered, causing text which should be escaped to not be. This could lead to an XSS attack.</td><td>V2: 4
V3: 6.1</td><td>go:golang.org/x/net<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201224014010-6772e930b67b</td><td>0.13.0</td></tr></table></td><td>Aug 2, 2023
05:30:20</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2023-6129</td><td>Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used. This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue.</td><td>V2: 4
V3: 6.5</td><td>openssl/libssl3
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>3.0.11-1~deb12u2</td><td>3.0.13-1~deb12u1</td></tr>
</table></td><td>May 3, 2024
09:15:21</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2022-27191</td><td>golang.org/x/crypto/ssh Denial of service via crafted Signer
The golang.org/x/crypto/ssh package before 0.0.0-20220314234659-1baeb1ce4c0b for Go allows an attacker to crash a server in certain circumstances involving AddHostKey.</td><td>V2: 4.3
V3: 7.5</td><td>go:golang.org/x/crypto<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201002170205-7f63de1d35b0</td><td>0.0.0-20220314234659-1baeb1ce4c0b</td></tr></table></td><td>Mar 18, 2022 08:01:02</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2023-47108</td><td>otelgrpc DoS vulnerability due to unbound cardinality metrics
Summary
The grpc Unary Server Interceptor [opentelemetry-go-contrib/instrumentation/google.golang.org/grpc/otelgrpc/interceptor.go](https://github.com/open-telemetry/opentelemetry-go-contrib/blob/9d4eb7e7706038b07d33f83f76afbe13f53d171d/instrumentation/google.golang.org/grpc/otelgrpc/interceptor.go#L327)
```
// UnaryServerInterceptor returns a grpc.UnaryServerInterceptor suitable
// for use in a grpc.NewServer call.
func UnaryServerInterceptor(opts ...Option) grpc.UnaryServerInterceptor {
```
out of the box adds labels
- `net.peer.sock.addr`
- `net.peer.sock.port`
that have unbound cardinality. It leads to the server's potential memory exhaustion when many malicious requests are sent.
Details
An attacker can easily flood the peer address and port for requests.
PoC
Apply the attached patch to the example and run the client multiple times. Observe how each request will create a unique histogram and how the memory consumption increases during it.
Impact
In order to be affected, the program has to configure a metrics pipeline, use [UnaryServerInterceptor](https://github.com/open-telemetry/opentelemetry-go-contrib/blob/9d4eb7e7706038b07d33f83f76afbe13f53d171d/instrumentation/google.golang.org/grpc/otelgrpc/interceptor.go#L327), and does not filter any client IP address and ports via middleware or proxies, etc.</td><td>V2: 7
V3: 7.5</td><td>go:go.opentelemetry.io/contrib/instrumentation/google.golang.org/grpc/otelgrpc<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.42.0</td><td>0.46.0</td></tr></table></td><td>Nov 12, 2023
10:55:39</td></tr>
</table>

Name	Description	Score	Packages	Published at
	### Others It is similar to already reported vulnerabilities. * [GHSA-rcjv-mgp8-qvmr](https://github.com/open-telemetry/opentelemetry-go-contrib/security/advisories/GHSA-rcjv-mgp8-qvmr) ([open-telemetry/opentelemetry-go-contrib](https://github.com/open-telemetry/opentelemetry-go-contrib)) - [GHSA-5r5m-65gx-7vrh](https://github.com/open-telemetry/opentelemetry-go-contrib/security/advisories/GHSA-5r5m-65gx-7vrh "GHSA-5r5m-65gx-7vrh") ([open-telemetry/opentelemetry-go-contrib](https://github.com/open-telemetry/opentelemetry-go-contrib)) - [GHSA-cg3q-j54f-5p7p](https://github.com/advisories/GHSA-cg3q-j54f-5p7p "GHSA-cg3q-j54f-5p7p") ([prometheus/client_golang](https://github.com/prometheus/client_golang)) ### Workaround for affected versions As a workaround to stop being affected, a view removing the attributes can be used. The other possibility is to disable grpc metrics instrumentation by passing [`otelgrpc.WithMeterProvider`](https://github.com/open-telemetry/opentelemetry-go-contrib/blob/instrumentation/google.golang.org/grpc/otelgrpc/v0.45.0/instrumentation/google.golang.org/grpc/otelgrpc/config.go#L138) option with [`noop.NewMeterProvider`](https://pkg.go.dev/go.opentelemetry.io/otel/metric/noop#NewMeterProvider). ### Solution provided by upgrading In PR [#4322](https://github.com/open-telemetry/opentelemetry-go-contrib/pull/4322), to be released with v0.46.0, the attributes were removed. ### References - [#4322](https://github.com/open-telemetry/opentelemetry-go-contrib/pull/4322)			

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>GHSA-m425-mq94-257g</td><td>gRPC-Go HTTP/2 Rapid Reset vulnerability
Impact
In affected releases of gRPC-Go, it is possible for an attacker to send HTTP/2 requests, cancel them, and send subsequent requests, which is valid by the HTTP/2 protocol, but would cause the gRPC-Go server to launch more concurrent method handlers than the configured maximum stream limit.
Patches
This vulnerability was addressed by #6703 and has been included in patch releases: 1.56.3, 1.57.1, 1.58.3. It is also included in the latest release, 1.59.0.
Along with applying the patch, users should also ensure they are using the `grpc.MaxConcurrentStreams` server option to apply a limit to the server's resources used for any single connection.
Workarounds
None.
References
#6703</td><td>V2: 7
V3: 7.5</td><td>go:google.golang.org/grpc<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.57.0</td><td>1.56.3;1.57.1;1.58.3</td></tr></table></td><td>Oct 25, 2023
05:17:37</td></tr>
<tr><td>CVE-2023-7008</td><td>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.</td><td>V2: 4
V3: 5.9</td><td>systemd<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>249.11-0ubuntu3.12</td><td>N/A</td></tr></table>systemd/libsystemd0<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>249.11-0ubuntu3.12</td><td>N/A</td></tr><tr><td>245.4-4ubuntu3.23</td><td>N/A</td></tr></table>systemd/libudev1<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>245.4-4ubuntu3.23</td><td>N/A</td></tr><tr><td>249.11-0ubuntu3.12</td><td>N/A</td></tr></table>...(4 packages)</td><td>May 22, 2024
01:16:10</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-6387</td><td>A security regression (CVE-2006-5051) was discovered in OpenSSH's server (sshd). There is a race condition which can lead sshd to handle some signals in an unsafe manner. An unauthenticated, remote attacker may be able to trigger it by failing to authenticate within a set time period.</td><td>V2: 7
V3: 8.1</td><td>openssh/openssh-client
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:8.9p1-3ubuntu0.7</td><td>1:8.9p1-3ubuntu0.10</td></tr></table>
openssh/openssh-server
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:8.9p1-3ubuntu0.7</td><td>1:8.9p1-3ubuntu0.10</td></tr></table>
openssh/openssh-sftp-server
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:8.9p1-3ubuntu0.7</td><td>1:8.9p1-3ubuntu0.10</td></tr></table></td><td>Jul 29, 2024
10:15:08</td></tr>
<tr><td>CVE-2023-39325</td><td>HTTP/2 rapid reset can cause excessive work in net/http
A malicious HTTP/2 client which rapidly creates requests and immediately resets them can cause excessive server resource consumption. While the total number of requests is bounded by the http2.Server.MaxConcurrentStreams setting, resetting an in-progress request allows the attacker to create a new request while the existing one is still executing.
With the fix applied, HTTP/2 servers now bound the number of simultaneously executing handler goroutines to the stream concurrency limit (MaxConcurrentStreams). New requests arriving when at the limit (which can only happen after the client has reset an existing, in-flight request) will be queued until a handler exits. If the request queue grows too large, the server will terminate the connection.
This issue is also fixed in golang.org/x/net/http2 for users manually configuring HTTP/2.
The default stream concurrency limit is 250 streams (requests) per HTTP/2 connection. This value may be adjusted using the golang.org/x/net/http2 package; see the Server.MaxConcurrentStreams setting and the ConfigureServer function.</td><td>V2: 7
V3: 7.5</td><td>go:golang.org/x/net
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.14.0</td><td>0.17.0</td></tr><tr><td>0.0.0-20201224014010-6772e930b67b</td><td>0.17.0</td></tr></table></td><td>Oct 11, 2023
04:35:43</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2022-29526</td><td>golang.org/x/sys/unix has Incorrect privilege reporting in syscall
Go before 1.17.10 and 1.18.x before 1.18.2 has Incorrect Privilege Reporting in syscall. When called with a non-zero flags parameter, the Faccessat function could incorrectly report that a file is accessible.
Specific Go Packages Affected
golang.org/x/sys/unix</td><td>V2: 5
V3: 5.3</td><td>go:golang.org/x/sys<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20210217105451-b926d437f341</td><td>0.0.0-20220412211240-33da011f77ad</td></tr></table></td><td>Jun 23, 2022
08:00:30</td></tr>
<tr><td>CVE-2022-27664</td><td>golang.org/x/net/http2 Denial of Service vulnerability
In net/http in Go before 1.18.6 and 1.19.x before 1.19.1, attackers can cause a denial of service because an HTTP/2 connection can hang during closing if shutdown were preempted by a fatal error.</td><td>V2: 7
V3: 7.5</td><td>go:golang.org/x/net<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201224014010-6772e930b67b</td><td>0.0.0-20220906165146-f3363e06e74c</td></tr></table></td><td>Sep 6, 2022
08:01:51</td></tr>
<tr><td>GHSA-c5pj-mqfh-rvc3</td><td>Withdrawn: Runc allows an arbitrary systemd property to be injected
Withdrawn Advisory
This advisory has been withdrawn because it was incorrectly attributed to runc. Please see the issue [here](https://github.com/opencontainers/runc/issues/4263) for more information.
Original Description
A flaw was found in cri-o, where an arbitrary systemd property can be injected via a Pod annotation. Any user who can create a pod with an arbitrary annotation may perform an arbitrary action on the host system. This issue has its root in how runc handles Config Annotations lists.</td><td>V2: 7
V3: 7.2</td><td>go:github.com/opencontainers/runc<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.1.12</td><td>1.2.0-rc.1</td></tr></table></td><td>Apr 26, 2024
02:30:34</td></tr>
</table>

Name	Description	Score	Packages	Published at
CVE-2023-45288	net/http, x/net/http2: close connections when receiving too many headers An attacker may cause an HTTP/2 endpoint to read arbitrary amounts of header data by sending an excessive number of CONTINUATION frames. Maintaining HPACK state requires parsing and processing all HEADERS and CONTINUATION frames on a connection. When a request's headers exceed MaxHeaderBytes, no memory is allocated to store the excess headers, but they are still parsed. This permits an attacker to cause an HTTP/2 endpoint to read arbitrary amounts of header data, all associated with a request which is going to be rejected. These headers can include Huffman-encoded data which is significantly more expensive for the receiver to decode than for an attacker to send. The fix sets a limit on the amount of excess header frames we will process before closing a connection.	**V2:** 4 **V3:** 5.3	go:golang.org/x/net **Impacted Version** / **Fixed Version** 0.0.0-20201224014010-6772e930b67b / 0.23.0 0.14.0 / 0.23.0 0.17.0 / 0.23.0	Apr 4, 2024 05:30:32
CVE-2024-34397	An issue was discovered in GNOME GLib before 2.78.5, and 2.79.x and 2.80.x before 2.80.1. When a GDBus-based client subscribes to signals from a trusted system service such as NetworkManager on a shared computer, other users of the same computer can send spoofed D-Bus signals that the GDBus-based client will wrongly interpret as having been sent by the trusted system service. This could lead to the GDBus-based client behaving incorrectly, with an application-dependent impact.	**V2:** 1 **V3:** 3.8	glib2.0/libglib2.0-0 **Impacted Version** / **Fixed Version** 2.72.4-0ubuntu2.2 / 2.72.4-0ubuntu2.3	Jun 10, 2024 02:15:34
CVE-2024-26461	Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/k5sealv3.c.	**V2:** 7 **V3:** 7.5	krb5/libgssapi-krb5-2 **Impacted Version** / **Fixed Version** 1.19.2-2ubuntu0.3 / N/A krb5/libk5crypto3 **Impacted Version** / **Fixed Version** 1.19.2-2ubuntu0.3 / N/A krb5/libkrb5-3 **Impacted Version** / **Fixed Version** 1.19.2-2ubuntu0.3 / N/A ...(4 packages)	Aug 14, 2024 12:35:10

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-2511</td><td>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.</td><td><b>V2:</b> 1
<b>V3:</b> 3.7</td><td>openssl
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.17</td></tr></table>
openssl/libssl3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.0.2-0ubuntu1.15</td><td>3.0.2-0ubuntu1.17</td></tr></table></td><td>May 3, 2024
09:15:21</td></tr>
<tr><td>CVE-2016-1585</td><td>In all versions of AppArmor mount rules are accidentally widened when compiled.</td><td><b>V2:</b> 7.5
<b>V3:</b> 9.8</td><td>apparmor/libapparmor1
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.0.4-2ubuntu2.3</td><td>N/A</td></tr></table></td><td>Nov 6, 2023
09:29:58</td></tr>
<tr><td>CVE-2022-41723</td><td>golang.org/x/net vulnerable to Uncontrolled Resource Consumption
A maliciously crafted HTTP/2 stream could cause excessive CPU consumption in the HPACK decoder, sufficient to cause a denial of service from a small number of small requests.</td><td><b>V2:</b> 7
<b>V3:</b> 7.5</td><td>go:golang.org/x/net
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.0.0-20201224014010-6772e930b67b</td><td>0.7.0</td></tr></table></td><td>Feb 17, 2023
09:00:02</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2023-5678</td><td>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 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.</td><td>V2: 4
V3: 5.3</td><td>openssl/libssl3<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.0.11-1~deb12u2</td><td>3.0.13-1~deb12u1</td></tr></table></td><td>May 1, 2024
02:15:12</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr>
<td>CVE-2023-48795</td>
<td>Prefix Truncation Attack against ChaCha20-Poly1305 and Encrypt-then-MAC aka Terrapin
Summary
Terrapin is a prefix truncation attack targeting the SSH protocol. More precisely, Terrapin breaks the integrity of SSH's secure channel. By carefully adjusting the sequence numbers during the handshake, an attacker can remove an arbitrary amount of messages sent by the client or server at the beginning of the secure channel without the client or server noticing it.
Mitigations
To mitigate this protocol vulnerability, OpenSSH suggested a so-called "strict kex" which alters the SSH handshake to ensure a Man-in-the-Middle attacker cannot introduce unauthenticated messages as well as convey sequence number manipulation across handshakes.
Warning: To take effect, both the client and server must support this countermeasure.
As a stop-gap measure, peers may also (temporarily) disable the affected algorithms and use unaffected alternatives like AES-GCM instead until patches are available.
Details
The SSH specifications of ChaCha20-Poly1305 (chacha20-poly1305@openssh.com) and Encrypt-then-MAC (*-etm@openssh.com MACs) are vulnerable against an arbitrary prefix truncation attack (a.k.a. Terrapin attack). This allows for an extension negotiation downgrade by stripping the SSH_MSG_EXT_INFO sent after the first message after SSH_MSG_NEWKEYS, downgrading security, and disabling attack countermeasures in some versions of OpenSSH. When targeting Encrypt-then-MAC, this attack requires the use of a CBC cipher to be practically exploitable due to the internal workings of the cipher mode. Additionally, this novel attack technique can be used to exploit previously unexploitable implementation flaws in a Man-in-the-Middle scenario.</td>
<td>V2: 4
V3: 5.9</td>
<td>go:golang.org/x/crypto
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>0.12.0</td><td>0.17.0</td></tr>
<tr><td>0.0.0-20201002170205-7f63de1d35b0</td><td>0.17.0</td></tr>
</table>
</td>
<td>Dec 18, 2023
02:22:09</td>
</tr>
</table>

Name	Description	Score	Packages	Published at
	The attack works by an attacker injecting an arbitrary number of SSH_MSG_IGNORE messages during the initial key exchange and consequently removing the same number of messages just after the initial key exchange has concluded. This is possible due to missing authentication of the excess SSH_MSG_IGNORE messages and the fact that the implicit sequence numbers used within the SSH protocol are only checked after the initial key exchange. In the case of ChaCha20-Poly1305, the attack is guaranteed to work on every connection as this cipher does not maintain an internal state other than the message's sequence number. In the case of Encrypt-Then-MAC, practical exploitation requires the use of a CBC cipher; while theoretical integrity is broken for all ciphers when using this mode, message processing will fail at the application layer for CTR and stream ciphers. For more details see https://terrapin-attack.com. ### Impact This attack targets the specification of ChaCha20-Poly1305 (chacha20-poly1305@openssh.com) and Encrypt-then-MAC (*-etm@openssh.com), which are widely adopted by well-known SSH implementations and can be considered de-facto standard. These algorithms can be practically exploited; however, in the case of Encrypt-Then-MAC, we additionally require the use of a CBC cipher. As a consequence, this attack works against all well-behaving SSH implementations supporting either of those algorithms and can be used to downgrade (but not fully strip) connection security in case SSH extension negotiation (RFC8308) is supported. The attack may also enable attackers to exploit certain implementation flaws in a man-in-the-middle (MitM) scenario.			

Name	Description	Score	Packages	Impacted Version	Fixed Version	Published at
CVE-2022-27943	libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as demonstrated by nm-new.	V2: 4.3 V3: 5.5	gcc-12/gcc-12-base	12.3.0-1ubuntu1~22.04	N/A	Nov 6, 2023 10:45:32
			gcc-12/libgcc-s1	12.3.0-1ubuntu1~22.04	N/A	
			gcc-12/libstdc++6	12.3.0-1ubuntu1~22.04	N/A	
CVE-2016-2781	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.	V2: 2.1 V3: 6.5	coreutils	9.1-1	N/A	Nov 6, 2023 09:32:03
				8.30-3ubuntu2	N/A	
				8.32-4.1ubuntu1.2	N/A	
CVE-2017-18018	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.	V2: 1.9 V3: 4.7	coreutils	9.1-1	N/A	Jan 19, 2018 10:46:46
CVE-2019-1010022	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.	V2: 7.5 V3: 9.8	glibc/libc6	2.36-9+deb12u4	N/A	Aug 4, 2024 11:15:25
CVE-2017-11164	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.	V2: 7.8 V3: 7.5	pcre3/libpcre3	2:8.39-12ubuntu0.1	N/A	Nov 6, 2023 09:38:10
				2:8.39-13ubuntu0.22.04.1	N/A	

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2019-1010023</td><td>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.</td><td>V2: 6.8
V3: 5.4</td><td>glibc/libc6<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.36-9+deb12u4</td><td>N/A</td></tr></table></td><td>Aug 4, 2024
11:15:25</td></tr>
<tr><td>CVE-2024-0760</td><td>A malicious client can send many DNS messages over TCP, potentially causing the server to become unstable while the attack is in progress. The server may recover after the attack ceases. Use of ACLs will not mitigate the attack. This issue affects BIND 9 versions 9.18.1 through 9.18.27, 9.19.0 through 9.19.24, and 9.18.11-S1 through 9.18.27-S1.</td><td>V2: 7
V3: 7.5</td><td>bind9/bind9-dnsutils<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr></table>bind9/bind9-host<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr></table>bind9/bind9-libs<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1:9.18.18-0ubuntu0.22.04.2</td><td>1:9.18.28-0ubuntu0.22.04.1</td></tr></table>...(4 packages)</td><td>Aug 1, 2024
09:45:59</td></tr>
<tr><td>CVE-2022-3219</td><td>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.</td><td>V2: 1
V3: 3.3</td><td>gnupg2/dirmngr<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.2.27-3ubuntu2.1</td><td>N/A</td></tr></table>gnupg2/gnupg<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.2.27-3ubuntu2.1</td><td>N/A</td></tr></table>gnupg2/gnupg-l10n<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.2.27-3ubuntu2.1</td><td>N/A</td></tr></table>...(11 packages)</td><td>May 26, 2023
12:31:34</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td>CVE-2024-22189</td><td>QUIC's Connection ID Mechanism vulnerable to Memory Exhaustion Attack
An attacker can cause its peer to run out of memory by sending a large number of NEW_CONNECTION_ID frames that retire old connection IDs. The receiver is supposed to respond to each retirement frame with a RETIRE_CONNECTION_ID frame. The attacker can prevent the receiver from sending out (the vast majority of) these RETIRE_CONNECTION_ID frames by collapsing the peers congestion window (by selectively acknowledging received packets) and by manipulating the peer's RTT estimate.
I published a more detailed description of the attack and its mitigation in this blog post: https://seemann.io/posts/2024-03-19-exploiting-quics-connection-id-management/.
I also presented this attack in the IETF QUIC working group session at IETF 119: https://youtu.be /JqXtYcZAtIA?si=nJ31QKLBSTRXY35U&t=3683
There's no way to mitigate this attack, please update quic-go to a version that contains the fix.</td><td>V2: 7
V3: 7.5</td><td>go:github.com/quic-go/quic-go<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.37.4</td><td>0.42.0</td></tr></table></td><td>Apr 2, 2024
10:16:05</td></tr>
<tr><td>CVE-2024-4032</td><td>The “ipaddress” module contained incorrect information about whether certain IPv4 and IPv6 addresses were designated as “globally reachable” or “private”. This affected the is_private and is_global properties of the ipaddress.IPv4Address, ipaddress.IPv4Network, ipaddress.IPv6Address, and ipaddress.IPv6Network classes, where values wouldn’t be returned in accordance with the latest information from the IANA Special-Purpose Address Registries. CPython 3.12.4 and 3.13.0a6 contain updated information from these registries and thus have the intended behavior.</td><td>V2: 1
V3: 3.7</td><td>python3.10<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.5</td></tr></table>python3.10/libpython3.10-minimal<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.5</td></tr></table>python3.10/libpython3.10-stdlib<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>3.10.12-1~22.04.3</td><td>3.10.12-1~22.04.5</td></tr></table>...(4 packages)</td><td>Jul 28, 2024
10:15:10</td></tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr>
<td>CVE-2022-21698</td>
<td>Uncontrolled Resource Consumption in promhttp
This is the Go client library for Prometheus. It has two separate parts, one for instrumenting application code, and one for creating clients that talk to the Prometheus HTTP API. client_golang is the instrumentation library for Go applications in Prometheus, and the promhttp package in client_golang provides tooling around HTTP servers and clients.
Impact
HTTP server susceptible to a Denial of Service through unbounded cardinality, and potential memory exhaustion, when handling requests with non-standard HTTP methods.
Affected Configuration
In order to be affected, an instrumented software must
* Use any of `promhttp.InstrumentHandler*` middleware except `RequestsInFlight`.
* Do not filter any specific methods (e.g GET) before middleware.
* Pass metric with `method` label name to our middleware.
* Not have any firewall/LB/proxy that filters away requests with unknown `method`.
Patches
* https://github.com/prometheus/client_golang/pull/962
* https://github.com/prometheus/client_golang/pull/987
Workarounds
If you cannot upgrade to [v1.11.1 or above](https://github.com /prometheus/client_golang/releases/tag/v1.11.1), in order to stop being affected you can:
* Remove `method` label name from counter/gauge you use in the InstrumentHandler.
* Turn off affected promhttp handlers.
* Add custom middleware before promhttp handler that will sanitize the request method given by Go http.Request.
* Use a reverse proxy or web application firewall, configured to only allow a limited set of methods.
For more information</td>
<td>V2: 5
V3: 7.5</td>
<td>go:github.com/prometheus/client_golang
<table>
<tr><th>Impacted Version</th><th>Fixed Version</th></tr>
<tr><td>1.7.1</td><td>1.11.1</td></tr>
</table>
</td>
<td>Feb 16, 2022
05:26:35</td>
</tr>
</table>

<table>
<tr><th>Name</th><th>Description</th><th>Score</th><th>Packages</th><th>Published at</th></tr>
<tr><td></td><td>If you have any questions or comments about this advisory:
* Open an issue in https://github.com/prometheus/client_golang
* Email us at `prometheus-team@googlegroups.com`</td><td></td><td></td><td></td></tr>
<tr><td>CVE-2021-38561</td><td>golang.org/x/text/language Out-of-bounds Read vulnerability golang.org/x/text/language in golang.org/x/text before 0.3.7 can panic with an out-of-bounds read during BCP 47 language tag parsing. Index calculation is mishandled. If parsing untrusted user input, this can be used as a vector for a denial-of-service attack.</td><td>V2: 7
V3: 7.5</td><td>go:golang.org/x/text
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>0.3.5</td><td>0.3.7</td></tr></table></td><td>Dec 26, 2022
01:30:22</td></tr>
<tr><td>CVE-2024-37371</td><td>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.</td><td>V2: 4
V3: 6.5</td><td>krb5/libgssapi-krb5-2
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>1.19.2-2ubuntu0.4</td></tr></table>
krb5/libk5crypto3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>1.19.2-2ubuntu0.4</td></tr></table>
krb5/libkrb5-3
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>1.19.2-2ubuntu0.3</td><td>1.19.2-2ubuntu0.4</td></tr></table>
...(4 packages)</td><td>Jul 1, 2024
08:37:24</td></tr>
<tr><td>CVE-2016-20013</td><td>sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of service (CPU consumption) because the algorithm's runtime is proportional to the square of the length of the password.</td><td>V2: 5
V3: 7.5</td><td>glibc/libc-bin
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.35-0ubuntu3.7</td><td>N/A</td></tr><tr><td>2.31-0ubuntu9.16</td><td>N/A</td></tr></table>
glibc/libc6
<table><tr><th>Impacted Version</th><th>Fixed Version</th></tr><tr><td>2.31-0ubuntu9.16</td><td>N/A</td></tr><tr><td>2.35-0ubuntu3.7</td><td>N/A</td></tr></table></td><td>Mar 3, 2022
11:43:19</td></tr>
</table>

Name	Description	Score	Packages	Published at
CVE-2023-27043	The email module of Python through 3.11.3 incorrectly parses e-mail addresses that contain a special character. The wrong portion of an RFC2822 header is identified as the value of the addr-spec. In some applications, an attacker can bypass a protection mechanism in which application access is granted only after verifying receipt of e-mail to a specific domain (e.g., only @company.example.com addresses may be used for signup). This occurs in email/_parseaddr.py in recent versions of Python.	**V2:** 4 **V3:** 5.3	python3.10 **Impacted Version**: 3.10.12-1~22.04.3 — **Fixed Version**: N/A python3.10/libpython3.10-minimal **Impacted Version**: 3.10.12-1~22.04.3 — **Fixed Version**: N/A python3.10/libpython3.10-stdlib **Impacted Version**: 3.10.12-1~22.04.3 — **Fixed Version**: N/A ...(4 packages)	Feb 26, 2024 11:27:45
CVE-2024-26462	Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.	**V2:** 7 **V3:** 7.5	krb5/libgssapi-krb5-2 **Impacted Version**: 1.19.2-2ubuntu0.3 — **Fixed Version**: N/A krb5/libk5crypto3 **Impacted Version**: 1.19.2-2ubuntu0.3 — **Fixed Version**: N/A krb5/libkrb5-3 **Impacted Version**: 1.19.2-2ubuntu0.3 — **Fixed Version**: N/A ...(4 packages)	May 14, 2024 11:09:01

Appendix (Full package list) (Show full list of packages)

CVE-2024-5535

openssl

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

openssl/libssl3

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

CVE-2024-4741

openssl

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

openssl/libssl3

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

CVE-2024-0397

python3.10

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

python3.10/libpython3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

python3.10/libpython3.10-stdlib

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

python3.10/python3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

CVE-2023-6597

python3.10

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

python3.10/libpython3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

python3.10/libpython3.10-stdlib

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

python3.10/python3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

CVE-2024-4603

openssl

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

openssl/libssl3

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

CVE-2024-1975

bind9/bind9-dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-host

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-libs

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

CVE-2024-2236

libgcrypt20

Impacted Version	Fixed Version
1.9.4-3ubuntu3	N/A
1.8.5-5ubuntu1.1	N/A

CVE-2024-33601

glibc/libc-bin

Impacted Version	Fixed Version
2.35-0ubuntu3.7	2.35-0ubuntu3.8

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	2.36-9+deb12u7
2.35-0ubuntu3.7	2.35-0ubuntu3.8

CVE-2023-50495

ncurses/libncurses6

Impacted Version	Fixed Version
6.3-2ubuntu0.1	N/A
6.2-0ubuntu2.1	N/A

ncurses/libncursesw6

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

ncurses/libtinfo6

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

ncurses/ncurses-base

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

ncurses/ncurses-bin

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

CVE-2021-31525

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.0.0-20210428140749-89ef3d95e781

CVE-2023-26604

systemd/libsystemd0

Impacted Version	Fixed Version
245.4-4ubuntu3.23	N/A

systemd/libudev1

Impacted Version	Fixed Version
245.4-4ubuntu3.23	N/A

CVE-2019-9192

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	N/A

CVE-2024-26458

krb5/libgssapi-krb5-2

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libk5crypto3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libkrb5-3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libkrb5support0

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

CVE-2024-0450

python3.10

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

python3.10/libpython3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

python3.10/libpython3.10-stdlib

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

python3.10/python3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.4

CVE-2023-6237

openssl/libssl3

Impacted Version	Fixed Version

Impacted Version	Fixed Version
3.0.11-1~deb12u2	3.0.13-1~deb12u1

CVE-2022-40735

openssl

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.16

openssl/libssl3

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.16

CVE-2020-29652

go:golang.org/x/crypto

Impacted Version	Fixed Version
0.0.0-20201002170205-7f63de1d35b0	0.0.0-20201216223049-8b5274cf687f

CVE-2018-20796

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	N/A

CVE-2022-41717

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.4.0

CVE-2021-33194

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.0.0-20210520170846-37e1c6afe023

CVE-2024-7264

curl

Impacted Version	Fixed Version

curl/libcurl4

Impacted Version	Fixed Version

Impacted Version	Fixed Version
7.81.0-1ubuntu1.16	7.81.0-1ubuntu1.17

Impacted Version	Fixed Version
7.81.0-1ubuntu1.16	7.81.0-1ubuntu1.17

CVE-2024-33600

glibc/libc-bin

Impacted Version	Fixed Version
2.35-0ubuntu3.7	2.35-0ubuntu3.8

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	2.36-9+deb12u7
2.35-0ubuntu3.7	2.35-0ubuntu3.8

CVE-2024-4076

bind9/bind9-dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-host

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-libs

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

CVE-2023-45918

ncurses/libncurses6

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

ncurses/libncursesw6

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

ncurses/libtinfo6

Impacted Version	Fixed Version
6.3-2ubuntu0.1	N/A
6.2-0ubuntu2.1	N/A

ncurses/ncurses-base

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

ncurses/ncurses-bin

Impacted Version	Fixed Version
6.2-0ubuntu2.1	N/A
6.3-2ubuntu0.1	N/A

CVE-2021-43565

go:golang.org/x/crypto

Impacted Version	Fixed Version
0.0.0-20201002170205-7f63de1d35b0	0.0.0-20211202192323-5770296d904e

CVE-2023-49295

go:github.com/quic-go/quic-go

Impacted Version	Fixed Version
0.37.4	0.40.1;0.39.4;0.38.2;0.37.7

CVE-2022-4899

libzstd/libzstd1

Impacted Version	Fixed Version
1.4.8+dfsg-3build1	N/A

CVE-2024-0727

openssl/libssl3

Impacted Version	Fixed Version
3.0.11-1~deb12u2	3.0.13-1~deb12u1

CVE-2023-44487

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.17.0
0.14.0	0.17.0

go:google.golang.org/grpc

Impacted Version	Fixed Version
1.57.0	1.58.3;1.57.1;1.56.3

CVE-2022-32149

go:golang.org/x/text

Impacted Version	Fixed Version
0.3.5	0.3.8

CVE-2023-29383

shadow/login

Impacted Version	Fixed Version
1:4.8.1-2ubuntu2.2	N/A
1:4.8.1-1ubuntu5.20.04.5	N/A

shadow/passwd

Impacted Version	Fixed Version
1:4.8.1-1ubuntu5.20.04.5	N/A
1:4.8.1-2ubuntu2.2	N/A

CVE-2024-28180

go:gopkg.in/square/go-jose.v2

Impacted Version	Fixed Version
2.6.0	N/A

CVE-2024-24786

go:google.golang.org/protobuf

Impacted Version	Fixed Version
1.25.0	1.33.0
1.31.0	1.33.0

CVE-2019-1010024

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	N/A

CVE-2024-1737

bind9/bind9-dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-host

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-libs

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

CVE-2024-2961

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	2.36-9+deb12u6

CVE-2019-1010025

glibc/libc6

Impacted Version	Fixed Version

Impacted Version	Fixed Version
2.36-9+deb12u4	N/A

CVE-2024-37370

krb5/libgssapi-krb5-2

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

krb5/libk5crypto3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

krb5/libkrb5-3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

krb5/libkrb5support0

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

CVE-2024-33602

glibc/libc-bin

Impacted Version	Fixed Version
2.35-0ubuntu3.7	2.35-0ubuntu3.8

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	2.36-9+deb12u7
2.35-0ubuntu3.7	2.35-0ubuntu3.8

CVE-2020-36325

jansson/libjansson4

Impacted Version	Fixed Version
2.14-2	N/A

CVE-2024-33599

glibc/libc-bin

Impacted Version	Fixed Version
2.35-0ubuntu3.7	2.35-0ubuntu3.8

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	2.36-9+deb12u7
2.35-0ubuntu3.7	2.35-0ubuntu3.8

CVE-2023-3978

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.13.0

CVE-2023-6129

openssl/libssl3

Impacted Version	Fixed Version
3.0.11-1~deb12u2	3.0.13-1~deb12u1

CVE-2022-27191

go:golang.org/x/crypto

Impacted Version	Fixed Version
0.0.0-20201002170205-7f63de1d35b0	0.0.0-20220314234659-1baeb1ce4c0b

CVE-2023-47108

go:go.opentelemetry.io/contrib/instrumentation/google.golang.org/grpc/otelgrpc

Impacted Version	Fixed Version
0.42.0	0.46.0

GHSA-m425-mq94-257g

go:google.golang.org/grpc

Impacted Version	Fixed Version
1.57.0	1.56.3;1.57.1;1.58.3

CVE-2023-7008

systemd

Impacted Version	Fixed Version
249.11-0ubuntu3.12	N/A

systemd/libsystemd0

Impacted Version	Fixed Version
249.11-0ubuntu3.12	N/A
245.4-4ubuntu3.23	N/A

systemd/libudev1

Impacted Version	Fixed Version
245.4-4ubuntu3.23	N/A
249.11-0ubuntu3.12	N/A

systemd/udev

Impacted Version	Fixed Version
249.11-0ubuntu3.12	N/A

CVE-2024-6387

openssh/openssh-client

openssh/openssh-server

openssh/openssh-sftp-server

Impacted Version	Fixed Version
1:8.9p1-3ubuntu0.7	1:8.9p1-3ubuntu0.10

Impacted Version	Fixed Version
1:8.9p1-3ubuntu0.7	1:8.9p1-3ubuntu0.10

Impacted Version	Fixed Version
1:8.9p1-3ubuntu0.7	1:8.9p1-3ubuntu0.10

CVE-2023-39325

go:golang.org/x/net

Impacted Version	Fixed Version
0.14.0	0.17.0
0.0.0-20201224014010-6772e930b67b	0.17.0

CVE-2022-29526

go:golang.org/x/sys

Impacted Version	Fixed Version
0.0.0-20210217105451-b926d437f341	0.0.0-20220412211240-33da011f77ad

CVE-2022-27664

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.0.0-20220906165146-f3363e06e74c

GHSA-c5pj-mqfh-rvc3

go:github.com/opencontainers/runc

Impacted Version	Fixed Version
1.1.12	1.2.0-rc.1

CVE-2023-45288

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.23.0

Impacted Version	Fixed Version
0.14.0	0.23.0
0.17.0	0.23.0

CVE-2024-34397

glib2.0/libglib2.0-0

Impacted Version	Fixed Version
2.72.4-0ubuntu2.2	2.72.4-0ubuntu2.3

CVE-2024-26461

krb5/libgssapi-krb5-2

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libk5crypto3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libkrb5-3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libkrb5support0

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

CVE-2024-2511

openssl

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

openssl/libssl3

Impacted Version	Fixed Version
3.0.2-0ubuntu1.15	3.0.2-0ubuntu1.17

CVE-2016-1585

apparmor/libapparmor1

Impacted Version	Fixed Version
3.0.4-2ubuntu2.3	N/A

CVE-2022-41723

go:golang.org/x/net

Impacted Version	Fixed Version
0.0.0-20201224014010-6772e930b67b	0.7.0

CVE-2023-5678

openssl/libssl3

Impacted Version	Fixed Version
3.0.11-1~deb12u2	3.0.13-1~deb12u1

CVE-2023-48795

go:golang.org/x/crypto

Impacted Version	Fixed Version
0.12.0	0.17.0
0.0.0-20201002170205-7f63de1d35b0	0.17.0

CVE-2022-27943

gcc-12/gcc-12-base

Impacted Version	Fixed Version
12.3.0-1ubuntu1~22.04	N/A

gcc-12/libgcc-s1

Impacted Version	Fixed Version
12.3.0-1ubuntu1~22.04	N/A

gcc-12/libstdc++6

Impacted Version	Fixed Version
12.3.0-1ubuntu1~22.04	N/A

CVE-2016-2781

coreutils

Impacted Version	Fixed Version
9.1-1	N/A
8.30-3ubuntu2	N/A
8.32-4.1ubuntu1.2	N/A

CVE-2017-18018

coreutils

Impacted Version	Fixed Version
9.1-1	N/A

CVE-2019-1010022

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	N/A

CVE-2017-11164

pcre3/libpcre3

Impacted Version	Fixed Version
2:8.39-12ubuntu0.1	N/A
2:8.39-13ubuntu0.22.04.1	N/A

CVE-2019-1010023

glibc/libc6

Impacted Version	Fixed Version
2.36-9+deb12u4	N/A

CVE-2024-0760

bind9/bind9-dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-host

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/bind9-libs

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

bind9/dnsutils

Impacted Version	Fixed Version
1:9.18.18-0ubuntu0.22.04.2	1:9.18.28-0ubuntu0.22.04.1

CVE-2022-3219

gnupg2/dirmngr

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gnupg

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gnupg-l10n

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gnupg-utils

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gpg

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gpg-agent

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gpg-wks-client

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gpg-wks-server

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gpgconf

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gpgsm

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

gnupg2/gpgv

Impacted Version	Fixed Version
2.2.27-3ubuntu2.1	N/A

Impacted Version	Fixed Version
2.2.19-3ubuntu2.2	N/A

CVE-2024-22189

go:github.com/quic-go/quic-go

Impacted Version	Fixed Version
0.37.4	0.42.0

CVE-2024-4032

python3.10

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

python3.10/libpython3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

python3.10/libpython3.10-stdlib

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

python3.10/python3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	3.10.12-1~22.04.5

CVE-2022-21698

go:github.com/prometheus/client_golang

Impacted Version	Fixed Version
1.7.1	1.11.1

CVE-2021-38561

go:golang.org/x/text

Impacted Version	Fixed Version
0.3.5	0.3.7

CVE-2024-37371

krb5/libgssapi-krb5-2

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

krb5/libk5crypto3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

krb5/libkrb5-3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

krb5/libkrb5support0

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	1.19.2-2ubuntu0.4

CVE-2016-20013

glibc/libc-bin

Impacted Version	Fixed Version
2.35-0ubuntu3.7	N/A
2.31-0ubuntu9.16	N/A

glibc/libc6

Impacted Version	Fixed Version
2.31-0ubuntu9.16	N/A
2.35-0ubuntu3.7	N/A

CVE-2023-27043

python3.10

Impacted Version	Fixed Version
3.10.12-1~22.04.3	N/A

python3.10/libpython3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	N/A

python3.10/libpython3.10-stdlib

Impacted Version	Fixed Version
3.10.12-1~22.04.3	N/A

python3.10/python3.10-minimal

Impacted Version	Fixed Version
3.10.12-1~22.04.3	N/A

CVE-2024-26462

krb5/libgssapi-krb5-2

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libk5crypto3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libkrb5-3

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A

krb5/libkrb5support0

Impacted Version	Fixed Version
1.19.2-2ubuntu0.3	N/A