



HTTP/2 Rapid Reset Attack Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2023-44487
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-10 14:15:00 UTC
Updated	2024-02-02 15:40:00 UTC
Description	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset man

Risk And Classification

EPSS: 0.944500000 probability, percentile 0.999920000 (date 2026-04-01)

CISA KEV: Listed on 2023-10-10; due 2023-10-31; ransomware use Unknown

Problem Types: CWE-400

CISA Known Exploited Vulnerability

Vendor	IETF
Product	HTTP/2
Name	HTTP/2 Rapid Reset Attack Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	This vulnerability affects a common open-source component, third-party library, or protocol used by different products. For more information, please see: HTTP/2 Rapid Reset Vulnerability, CVE-2023-44487 CISA: https://www.cisa.gov/news-events/alerts/2023/10/10/http2-rapid-reset-vulnerability-cve-2023-44487 ; https://blog.cloudflare.com/technical-breakdown-http2-rapid-reset-ddos-attack/ ; https://nvd.nist.gov/vuln/detail/CVE-2023-44487

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	La
Application	Akka	Http Server	All	All	All	All
Application	Amazon	Opensearch Data Prepper	All	All	All	All
Application	Apache	Apisix	All	All	All	All
Application	Apache	Solr	All	All	All	All
Application	Apache	Tomcat	11.0.0	milestone1	All	All

Application	Apache	Tomcat	11.0.0	milestone10	All	All
Application	Apache	Tomcat	11.0.0	milestone11	All	All
Application	Apache	Tomcat	11.0.0	milestone2	All	All
Application	Apache	Tomcat	11.0.0	milestone3	All	All
Application	Apache	Tomcat	11.0.0	milestone4	All	All
Application	Apache	Tomcat	11.0.0	milestone5	All	All
Application	Apache	Tomcat	11.0.0	milestone6	All	All
Application	Apache	Tomcat	11.0.0	milestone7	All	All
Application	Apache	Tomcat	11.0.0	milestone8	All	All
Application	Apache	Tomcat	11.0.0	milestone9	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Traffic Server	All	All	All	All
Application	Apple	Swiftnio Http/2	All	All	All	All
Application	Caddyserver	Caddy	All	All	All	All
Application	Cisco	Connected Mobile Experiences	All	All	All	All
Application	Cisco	Crosswork Data Gateway	All	All	All	All
Application	Cisco	Crosswork Data Gateway	5.0	All	All	All
Application	Cisco	Crosswork Zero Touch Provisioning	All	All	All	All
Application	Cisco	Data Center Network Manager	-	All	All	All
Application	Cisco	Enterprise Chat And Email	-	All	All	All
Application	Cisco	Expressway	All	All	All	All
Application	Cisco	Firepower Threat Defense	All	All	All	All
Operating System	Cisco	Fog Director	All	All	All	All
Operating System	Cisco	Ios Xe	All	All	All	All
Operating System	Cisco	Ios Xr	All	All	All	All
Application	Cisco	IoT Field Network Director	All	All	All	All
Hardware	Cisco	Nexus 3016	-	All	All	All
Hardware	Cisco	Nexus 3016q	-	All	All	All
Hardware	Cisco	Nexus 3048	-	All	All	All
Hardware	Cisco	Nexus 3064	-	All	All	All
Hardware	Cisco	Nexus 3064-32t	-	All	All	All
Hardware	Cisco	Nexus 3064-t	-	All	All	All
Hardware	Cisco	Nexus 3064-x	-	All	All	All

Hardware	Cisco	Nexus 3064t	-	All	All	All
Hardware	Cisco	Nexus 3064x	-	All	All	All
Hardware	Cisco	Nexus 3100	-	All	All	All
Hardware	Cisco	Nexus 3100-v	-	All	All	All
Hardware	Cisco	Nexus 3100-z	-	All	All	All
Hardware	Cisco	Nexus 3100v	-	All	All	All
Hardware	Cisco	Nexus 31108pc-v	-	All	All	All
Hardware	Cisco	Nexus 31108pv-v	-	All	All	All
Hardware	Cisco	Nexus 31108tc-v	-	All	All	All
Hardware	Cisco	Nexus 31128pq	-	All	All	All
Hardware	Cisco	Nexus 3132c-z	-	All	All	All
Hardware	Cisco	Nexus 3132q	-	All	All	All
Hardware	Cisco	Nexus 3132q-v	-	All	All	All
Hardware	Cisco	Nexus 3132q-x	-	All	All	All
Hardware	Cisco	Nexus 3132q-xl	-	All	All	All
Hardware	Cisco	Nexus 3132q-x/3132q-xl	-	All	All	All
Hardware	Cisco	Nexus 3164q	-	All	All	All
Hardware	Cisco	Nexus 3172	-	All	All	All
Hardware	Cisco	Nexus 3172pq	-	All	All	All
Hardware	Cisco	Nexus 3172pq-xl	-	All	All	All
Hardware	Cisco	Nexus 3172pq/pq-xl	-	All	All	All
Hardware	Cisco	Nexus 3172tq	-	All	All	All
Hardware	Cisco	Nexus 3172tq-32t	-	All	All	All
Hardware	Cisco	Nexus 3172tq-xl	-	All	All	All
Hardware	Cisco	Nexus 3200	-	All	All	All
Hardware	Cisco	Nexus 3232	-	All	All	All
Hardware	Cisco	Nexus 3232c	-	All	All	All
Hardware	Cisco	Nexus 3232c	-	All	All	All
Hardware	Cisco	Nexus 3264c-e	-	All	All	All
Hardware	Cisco	Nexus 3264q	-	All	All	All
Hardware	Cisco	Nexus 3400	-	All	All	All
Hardware	Cisco	Nexus 3408-s	-	All	All	All
Hardware	Cisco	Nexus 34180yc	-	All	All	All
Hardware	Cisco	Nexus 34200yc-sm	-	All	All	All
Hardware	Cisco	Nexus 3432d-s	-	All	All	All
Hardware	Cisco	Nexus 3464c	-	All	All	All

Hardware	Cisco	Nexus 3500	-	All	All	All
Hardware	Cisco	Nexus 3524	-	All	All	All
Hardware	Cisco	Nexus 3524-x	-	All	All	All
Hardware	Cisco	Nexus 3524-xl	-	All	All	All
Hardware	Cisco	Nexus 3524-x/xl	-	All	All	All
Hardware	Cisco	Nexus 3548	-	All	All	All
Hardware	Cisco	Nexus 3548-x	-	All	All	All
Hardware	Cisco	Nexus 3548-xl	-	All	All	All
Hardware	Cisco	Nexus 3548-x/xl	-	All	All	All
Hardware	Cisco	Nexus 3600	-	All	All	All
Hardware	Cisco	Nexus 36180yc-r	-	All	All	All
Hardware	Cisco	Nexus 3636c-r	-	All	All	All
Hardware	Cisco	Nexus 9000v	-	All	All	All
Hardware	Cisco	Nexus 9200	-	All	All	All
Hardware	Cisco	Nexus 9200yc	-	All	All	All
Hardware	Cisco	Nexus 92160yc-x	-	All	All	All
Hardware	Cisco	Nexus 92160yc Switch	-	All	All	All
Hardware	Cisco	Nexus 9221c	-	All	All	All
Hardware	Cisco	Nexus 92300yc	-	All	All	All
Hardware	Cisco	Nexus 92300yc Switch	-	All	All	All
Hardware	Cisco	Nexus 92304qc	-	All	All	All
Hardware	Cisco	Nexus 92304qc Switch	-	All	All	All
Hardware	Cisco	Nexus 9232e	-	All	All	All
Hardware	Cisco	Nexus 92348gc-x	-	All	All	All
Hardware	Cisco	Nexus 9236c	-	All	All	All
Hardware	Cisco	Nexus 9236c Switch	-	All	All	All
Hardware	Cisco	Nexus 9272q	-	All	All	All
Hardware	Cisco	Nexus 9272q Switch	-	All	All	All
Hardware	Cisco	Nexus 9300	-	All	All	All
Hardware	Cisco	Nexus 93108tc-ex	-	All	All	All
Hardware	Cisco	Nexus 93108tc-ex-24	-	All	All	All
Hardware	Cisco	Nexus 93108tc-ex Switch	-	All	All	All
Hardware	Cisco	Nexus 93108tc-fx	-	All	All	All
Hardware	Cisco	Nexus 93108tc-fx-24	-	All	All	All
Hardware	Cisco	Nexus 93108tc-fx3h	-	All	All	All

Hardware	Cisco	Nexus 93108tc-fx3p	-	All	All	All
Hardware	Cisco	Nexus 93120tx	-	All	All	All
Hardware	Cisco	Nexus 93120tx Switch	-	All	All	All
Hardware	Cisco	Nexus 93128	-	All	All	All
Hardware	Cisco	Nexus 93128tx	-	All	All	All
Hardware	Cisco	Nexus 93128tx Switch	-	All	All	All
Hardware	Cisco	Nexus 9316d-gx	-	All	All	All
Hardware	Cisco	Nexus 93180lc-ex	-	All	All	All
Hardware	Cisco	Nexus 93180lc-ex Switch	-	All	All	All
Hardware	Cisco	Nexus 93180tc-ex	-	All	All	All
Hardware	Cisco	Nexus 93180yc-ex	-	All	All	All
Hardware	Cisco	Nexus 93180yc-ex-24	-	All	All	All
Hardware	Cisco	Nexus 93180yc-ex Switch	-	All	All	All
Hardware	Cisco	Nexus 93180yc-fx	-	All	All	All
Hardware	Cisco	Nexus 93180yc-fx-24	-	All	All	All
Hardware	Cisco	Nexus 93180yc-fx3	-	All	All	All
Hardware	Cisco	Nexus 93180yc-fx3h	-	All	All	All
Hardware	Cisco	Nexus 93180yc-fx3s	-	All	All	All
Hardware	Cisco	Nexus 93216tc-fx2	-	All	All	All
Hardware	Cisco	Nexus 93240tc-fx2	-	All	All	All
Hardware	Cisco	Nexus 93240yc-fx2	-	All	All	All
Hardware	Cisco	Nexus 9332c	-	All	All	All
Hardware	Cisco	Nexus 9332d-gx2b	-	All	All	All
Hardware	Cisco	Nexus 9332d-h2r	-	All	All	All
Hardware	Cisco	Nexus 9332pq	-	All	All	All
Hardware	Cisco	Nexus 9332pq Switch	-	All	All	All
Hardware	Cisco	Nexus 93360yc-fx2	-	All	All	All
Hardware	Cisco	Nexus 9336c-fx2	-	All	All	All
Hardware	Cisco	Nexus 9336c-fx2-e	-	All	All	All
Hardware	Cisco	Nexus 9336pq	-	All	All	All
Hardware	Cisco	Nexus 9336pq Aci	-	All	All	All
Hardware	Cisco	Nexus 9336pq Aci Spine	-	All	All	All
Hardware	Cisco	Nexus 9336pq Aci Spine Switch	-	All	All	All
Hardware	Cisco	Nexus 9348d-gx2a	-	All	All	All
Hardware	Cisco	Nexus 9348gc-fx3	-	All	All	All

Hardware	Cisco	Nexus 9348gc-fxp	-	All	All	All
Hardware	Cisco	Nexus 93600cd-gx	-	All	All	All
Hardware	Cisco	Nexus 9364c	-	All	All	All
Hardware	Cisco	Nexus 9364c-gx	-	All	All	All
Hardware	Cisco	Nexus 9364d-gx2a	-	All	All	All
Hardware	Cisco	Nexus 9372px	-	All	All	All
Hardware	Cisco	Nexus 9372px-e	-	All	All	All
Hardware	Cisco	Nexus 9372px-e Switch	-	All	All	All
Hardware	Cisco	Nexus 9372px Switch	-	All	All	All
Hardware	Cisco	Nexus 9372tx	-	All	All	All
Hardware	Cisco	Nexus 9372tx-e	-	All	All	All
Hardware	Cisco	Nexus 9372tx-e Switch	-	All	All	All
Hardware	Cisco	Nexus 9372tx Switch	-	All	All	All
Hardware	Cisco	Nexus 9396px	-	All	All	All
Hardware	Cisco	Nexus 9396px Switch	-	All	All	All
Hardware	Cisco	Nexus 9396tx	-	All	All	All
Hardware	Cisco	Nexus 9396tx Switch	-	All	All	All
Hardware	Cisco	Nexus 9408	-	All	All	All
Hardware	Cisco	Nexus 9432pq	-	All	All	All
Hardware	Cisco	Nexus 9500	-	All	All	All
Hardware	Cisco	Nexus 9500r	-	All	All	All
Hardware	Cisco	Nexus 9500 16-slot	-	All	All	All
Hardware	Cisco	Nexus 9500 4-slot	-	All	All	All
Hardware	Cisco	Nexus 9500 8-slot	-	All	All	All
Hardware	Cisco	Nexus 9500 Supervisor A	-	All	All	All
Hardware	Cisco	Nexus 9500 Supervisor A	-	All	All	All
Hardware	Cisco	Nexus 9500 Supervisor B	-	All	All	All
Hardware	Cisco	Nexus 9500 Supervisor B	-	All	All	All
Hardware	Cisco	Nexus 9504	-	All	All	All
Hardware	Cisco	Nexus 9504 Switch	-	All	All	All
Hardware	Cisco	Nexus 9508	-	All	All	All
Hardware	Cisco	Nexus 9508 Switch	-	All	All	All
Hardware	Cisco	Nexus 9516	-	All	All	All
Hardware	Cisco	Nexus 9516 Switch	-	All	All	All
Hardware	Cisco	Nexus 9536pq	-	All	All	All
Hardware	Cisco	Nexus 9636pq	-	All	All	All

Hardware	Cisco	Nexus 9716d-gx	-	All	All	All
Hardware	Cisco	Nexus 9736pq	-	All	All	All
Hardware	Cisco	Nexus 9800	-	All	All	All
Hardware	Cisco	Nexus 9804	-	All	All	All
Hardware	Cisco	Nexus 9808	-	All	All	All
Operating System	Cisco	Nx-os	All	All	All	All
Application	Cisco	Prime Access Registrar	All	All	All	All
Application	Cisco	Prime Cable Provisioning	All	All	All	All
Application	Cisco	Prime Infrastructure	All	All	All	All
Application	Cisco	Prime Network Registrar	All	All	All	All
Application	Cisco	Secure Dynamic Attributes Connector	All	All	All	All
Application	Cisco	Secure Malware Analytics	All	All	All	All
Hardware	Cisco	Secure Web Appliance	-	All	All	All
Operating System	Cisco	Secure Web Appliance Firmware	All	All	All	All
Application	Cisco	Telepresence Video Communication Server	All	All	All	All
Application	Cisco	Ultra Cloud Core - Policy Control Function	All	All	All	All
Application	Cisco	Ultra Cloud Core - Policy Control Function	2024.01.0	All	All	All
Application	Cisco	Ultra Cloud Core - Serving Gateway Function	All	All	All	All
Application	Cisco	Ultra Cloud Core - Session Management Function	All	All	All	All
Application	Cisco	Unified Attendant Console Advanced	-	All	All	All
Application	Cisco	Unified Contact Center Domain Manager	-	All	All	All
Application	Cisco	Unified Contact Center Enterprise	-	All	All	All
Application	Cisco	Unified Contact Center Enterprise - Live Data Server	All	All	All	All
Application	Cisco	Unified Contact Center Management Portal	-	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	12.0	All	All	All
Application	Dena	H2o	All	All	All	All
Application	Eclipse	Jetty	All	All	All	All
Application	Envoyproxy	Envoy	1.24.10	All	All	All
Application	Envoyproxy	Envoy	1.25.9	All	All	All
Application	Envoyproxy	Envoy	1.26.4	All	All	All
Application	Envoyproxy	Envoy	1.27.0	All	All	All
Application	F5	Big-ip Access Policy Manager	17.1.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All

Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	17.1.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	17.1.0	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Advanced Web Application Firewall	All	All	All	All
Application	F5	Big-ip Analytics	17.1.0	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	17.1.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	17.1.0	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	17.1.0	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	All	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	All	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	All	All	All	All
Application	F5	Big-ip Application Visibility And Reporting	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	17.1.0	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All

Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Carrier-grade Nat	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	17.1.0	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Ddos Hybrid Defender	All	All	All	All
Application	F5	Big-ip Domain Name System	17.1.0	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	17.1.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	17.1.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	17.1.0	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	17.1.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Next	20.0.1	All	All	All
Application	F5	Big-ip Next Service Proxy For Kubernetes	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	17.1.0	All	All	All

Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	17.1.0	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Ssl Orchestrator	All	All	All	All
Application	F5	Big-ip Webaccelerator	17.1.0	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Websafe	17.1.0	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Big-ip Websafe	All	All	All	All
Application	F5	Nginx	All	All	All	All
Application	F5	Nginx Ingress Controller	All	All	All	All
Application	F5	Nginx Ingress Controller	All	All	All	All
Application	F5	Nginx Plus	All	All	All	All
Application	F5	Nginx Plus	r29	-	All	All
Application	F5	Nginx Plus	r30	-	All	All
Application	Facebook	Proxygen	All	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Application	Golang	Go	All	All	All	All
Application	Golang	Http2	All	All	All	All
Application	Golang	Networking	All	All	All	All
Application	Grpc	Grpc	All	All	All	All
Application	Grpc	Grpc	1.57.0	-	All	All
Application	Grpc	Grpc	All	All	All	All
Application	Ietf	Http	2.0	All	All	All

Application	Istio	Istio	All	All	All	All
Application	Jenkins	Jenkins	All	All	All	All
Application	Jenkins	Jenkins	All	All	All	All
Application	Kazu-yamamoto	Http2	All	All	All	All
Application	Konghq	Kong Gateway	All	All	All	All
Application	Linecorp	Armeria	All	All	All	All
Application	Linkerd	Linkerd	2.13.0	All	All	All
Application	Linkerd	Linkerd	2.13.0	All	All	All
Application	Linkerd	Linkerd	2.13.1	All	All	All
Application	Linkerd	Linkerd	2.13.1	All	All	All
Application	Linkerd	Linkerd	2.14.0	All	All	All
Application	Linkerd	Linkerd	2.14.0	All	All	All
Application	Linkerd	Linkerd	2.14.1	All	All	All
Application	Linkerd	Linkerd	2.14.1	All	All	All
Application	Linkerd	Linkerd	All	All	All	All
Application	Linkerd	Linkerd	All	All	All	All
Application	Microsoft	.net	All	All	All	All
Application	Microsoft	Asp.net Core	All	All	All	All
Application	Microsoft	Azure Kubernetes Service	All	All	All	All
Application	Microsoft	Cbl-mariner	All	All	All	All
Application	Microsoft	Visual Studio 2022	All	All	All	All
Operating System	Microsoft	Windows 10 1607	All	All	All	All
Operating System	Microsoft	Windows 10 1607	All	All	All	All
Operating System	Microsoft	Windows 10 1809	All	All	All	All
Operating System	Microsoft	Windows 10 21h2	All	All	All	All
Operating System	Microsoft	Windows 10 22h2	All	All	All	All
Operating System	Microsoft	Windows 11 21h2	All	All	All	All
Operating System	Microsoft	Windows 11 22h2	All	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2019	-	All	All	All
Operating System	Microsoft	Windows Server 2022	-	All	All	All
Application	Netapp	Astra Control Center	-	All	All	All
Application	Netty	Netty	All	All	All	All
Application	Nghttp2	Nghttp2	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All
Application	Nodejs	Node.js	All	All	All	All

Application	nodejs	node.js	All	All	All	All
Application	Openresty	Openresty	All	All	All	All
Application	Projectcontour	Contour	All	All	All	All
Application	Redhat	3scale Api Management Platform	2.0	All	All	All
Application	Redhat	Advanced Cluster Management For Kubernetes	2.0	All	All	All
Application	Redhat	Advanced Cluster Security	3.0	All	All	All
Application	Redhat	Advanced Cluster Security	4.0	All	All	All
Application	Redhat	Ansible Automation Platform	2.0	All	All	All
Application	Redhat	Build Of Optaplanner	8.0	All	All	All
Application	Redhat	Build Of Quarkus	-	All	All	All
Application	Redhat	Ceph Storage	5.0	All	All	All
Application	Redhat	Cert-manager Operator For Red Hat Openshift	-	All	All	All
Application	Redhat	Certification For Red Hat Enterprise Linux	8.0	All	All	All
Application	Redhat	Certification For Red Hat Enterprise Linux	9.0	All	All	All
Application	Redhat	Cost Management	-	All	All	All
Application	Redhat	Cryostat	2.0	All	All	All
Application	Redhat	Decision Manager	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	9.0	All	All	All
Application	Redhat	Fence Agents Remediation Operator	-	All	All	All
Application	Redhat	Integration Camel For Spring Boot	-	All	All	All
Application	Redhat	Integration Camel K	-	All	All	All
Application	Redhat	Integration Service Registry	-	All	All	All
Application	Redhat	Jboss A-mq	7	All	All	All
Application	Redhat	Jboss A-mq Streams	-	All	All	All
Application	Redhat	Jboss Core Services	-	All	All	All
Application	Redhat	Jboss Data Grid	7.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	6.0.0	All	All	All
Application	Redhat	Jboss Enterprise Application Platform	7.0.0	All	All	All
Application	Redhat	Jboss Fuse	6.0.0	All	All	All
Application	Redhat	Jboss Fuse	7.0.0	All	All	All
Application	Redhat	Logging Subsystem For Red Hat Openshift	-	All	All	All
Application	Redhat	Machine Deletion Remediation Operator	-	All	All	All
Application	Redhat	Migration Toolkit For Applications	6.0	All	All	All

Application	Redhat	Migration Toolkit For Containers	-	All	All	All
Application	Redhat	Migration Toolkit For Virtualization	-	All	All	All
Application	Redhat	Network Observability Operator	-	All	All	All
Application	Redhat	Node Healthcheck Operator	-	All	All	All
Application	Redhat	Node Maintenance Operator	-	All	All	All
Application	Redhat	Openshift	-	All	All	All
Application	Redhat	Openshift Api For Data Protection	-	All	All	All
Application	Redhat	Openshift Container Platform	4.0	All	All	All
Application	Redhat	Openshift Container Platform Assisted Installer	-	All	All	All
Application	Redhat	Openshift Data Science	-	All	All	All
Application	Redhat	Openshift Developer Tools And Services	-	All	All	All
Application	Redhat	Openshift Dev Spaces	-	All	All	All
Application	Redhat	Openshift Distributed Tracing	-	All	All	All
Application	Redhat	Openshift Gitops	-	All	All	All
Application	Redhat	Openshift Pipelines	-	All	All	All
Application	Redhat	Openshift Sandboxed Containers	-	All	All	All
Application	Redhat	Openshift Secondary Scheduler Operator	-	All	All	All
Application	Redhat	Openshift Serverless	-	All	All	All
Application	Redhat	Openshift Service Mesh	2.0	All	All	All
Application	Redhat	Openshift Virtualization	4	All	All	All
Application	Redhat	Openstack Platform	16.1	All	All	All
Application	Redhat	Openstack Platform	16.2	All	All	All
Application	Redhat	Openstack Platform	17.1	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All
Application	Redhat	Quay	3.0.0	All	All	All
Application	Redhat	Run Once Duration Override Operator	-	All	All	All
Application	Redhat	Satellite	6.0	All	All	All
Application	Redhat	Self Node Remediation Operator	-	All	All	All
Application	Redhat	Service Interconnect	1.0	All	All	All
Application	Redhat	Service Telemetry Framework	1.5	All	All	All
Application	Redhat	Single Sign-on	7.0	All	All	All
Application	Redhat	Support For Spring Boot	-	All	All	All
Application	Redhat	Web Terminal	-	All	All	All
Application	Traefik	Traefik	All	All	All	All
Application	Traefik	Traefik	3.0.0	beta1	All	All

Application	Traefik	Traefik	3.0.0	beta2	All	All
Application	Traefik	Traefik	3.0.0	beta3	All	All
Application	Varnish Cache Project	Varnish Cache	All	All	All	All

References

Reference

myF5

[SECURITY] Fedora 39 Update: golang-1.21.3-1.fc39 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 37 Update: golang-1.20.10-3.fc37 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 38 Update: trafficserver-9.2.3-1.fc38 - package-announce - Fedora Mailing-Lists

github.com/icing/mod_h2/blob/0a864782af0a942aa2ad4ed960a6b32cd35bcf0a/mo...

How it works: The novel HTTP/2 'Rapid Reset' DDoS attack | Google Cloud Blog

Document non-impact of CVE-2023-44487 by raboof · Pull Request #10 · apache/httpd-site · GitHub

[SECURITY] Fedora 37 Update: mod_http2-2.0.25-1.fc37 - package-announce - Fedora Mailing-Lists

New 'HTTP/2 Rapid Reset' zero-day attack breaks DDoS records

Debian -- Security Information -- DSA-5521-1 tomcat10

github.com/apache/httpd/blob/afcdbeebff4b0c50ea26cdd16e178c0d1f24152/mo...

.NET 7 security vulnerability Kestrel Server HTTP/2 · oqtane/oqtane.framework · Discussion #3367 · GitHub

[SECURITY] [DLA 3638-1] h2o security update

Is Traefik vulnerable to CVE-2023-44487? - Traefik v2 (latest) - Traefik Labs Community Forum

[SECURITY] Fedora 38 Update: nghttp2-1.52.0-2.fc38 - package-announce - Fedora Mailing-Lists

oss-security - Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations

Stefan Eissing: "More details: httpd keeps a „mood“ counter for ea..." - chaos.social

Netty.news: Netty 4.1.100.Final released

[SECURITY] Fedora 38 Update: mcrouter-0.41.0.20231016-1.fc38 - package-announce - Fedora Mailing-Lists

h2 RST bug aka CVE-2023-44487 · Issue #2312 · haproxy/haproxy · GitHub

[SECURITY] Fedora 38 Update: nodejs18-18.18.2-1.fc38 - package-announce - Fedora Mailing-Lists

[debian-lts-announce] 20231119 [SECURITY] [DLA 3656-1] netty security update

[SECURITY] Fedora 37 Update: nodejs18-18.18.2-1.fc37 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 38 Update: trafficserver-9.2.3-1.fc38 - package-announce - Fedora Mailing-Lists

[security] Go 1.21.3 and Go 1.20.10 are released

[PATCH] HTTP/2: per-iteration stream handling limit

Limit max reset frames to mitigate HTTP/2 RST floods by ikhoon · Pull Request #5232 · line/armeria · GitHub

CVE-2023-44487 - HTTP/2 Rapid Reset Attack

[SECURITY] Fedora 38 Update: mcrouter-0.41.0.20231016-1.fc38 - package-announce - Fedora Mailing-Lists

Allow HTTP/2 rate control to mitigate HTTP/2 floods (CVE-2023-44487) · Issue #10670 · apache/httpd-project · GitHub

Allow HTTP/2 rate control to mitigate HTTP/2 floods (CVE-2023-44487) · Issue #10679 · eclipse/jetty.project · GitHub
How Linkerd became resilient to CVE-2023-44487, a HTTP/2 DDOS vulnerability, six months prior to its disclosure Linkerd
2242803 – (CVE-2023-44487) CVE-2023-44487 HTTP/2: Multiple HTTP/2 enabled web servers are vulnerable to a DDoS attack (Rapid Reset) · Issue #2242803 · apache/traffic-server · GitHub
[SECURITY] [DLA 3617-2] tomcat9 regression update
DSA-5570
[SECURITY] [DLA 3641-1] jetty9 security update
CVE-2023-44487 HTTP/2 Rapid Reset Attack Qualys Security Blog
Google mitigated the largest DDoS attack to date, peaking above 398M rps Hacker News
[SECURITY] Fedora 37 Update: nodejs18-18.18.2-1.fc37 - package-announce - Fedora Mailing-Lists
Pick a default for HTTP/2 server max concurrent streams · Issue #3337 · hyperium/hyper · GitHub
HTTP/2 Rapid Reset DDoS Mitigation · Issue #1986 · tempesta-tech/tempesta · GitHub
[SECURITY] Fedora 39 Update: nghttp2-1.55.1-4.fc39 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: folly-2023.10.16.00-1.fc37 - package-announce - Fedora Mailing-Lists
Is Cowboy affected by the HTTP/2 Rapid Reset attack? · Issue #1615 · ninenines/cowboy · GitHub
[SECURITY] Fedora 39 Update: nodejs20-20.8.1-1.fc39 - package-announce - Fedora Mailing-Lists
GitHub - bcdannyboy/CVE-2023-44487: Basic vulnerability scanning to see if web servers may be vulnerable to CVE-2023-44487
Resolve CVE-2023-44487 · Issue #16740 · etcd-io/etcd · GitHub
Biggest DDoSes of all time generated by protocol 0-day in HTTP/2 Ars Technica
initial draft of CVE-2023-44487 blog post by wmorgan · Pull Request #1695 · linkerd/website · GitHub
oss-security - CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
[SECURITY] Fedora 37 Update: nodejs20-20.8.1-1.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 39 Update: nodejs18-18.18.2-1.fc39 - package-announce - Fedora Mailing-Lists
Set stream limits for HTTP2 protocol - CVE CVE-2023-44487 by akshaysngupta · Pull Request #5826 · projectcontour/contour · GitHub
HTTP/2 Rapid Reset DDoS Attack · GitHub
CVE-2023-44487 HTTP/2 Vulnerability in NetApp Products NetApp Product Security
[http2] rapid reset attack by kazuho · Pull Request #3291 · h2o/h2o · GitHub
[SECURITY] Fedora 38 Update: nodejs20-20.8.1-1.fc38 - package-announce - Fedora Mailing-Lists
HTTP/2 Rapid Reset: deconstructing the record-breaking attack
Microsoft Security Advisory CVE-2023-44487: .NET Denial of Service Vulnerability · Issue #277 · dotnet/announcements · GitHub
Prevent rapid reset http2 DOS on API server by enj · Pull Request #121120 · kubernetes/kubernetes · GitHub
http: Fix CVE CVE-2023-44487 by phlax · Pull Request #30055 · envoyproxy/envoy · GitHub
HTTP/2 Rapid Reset (CVE-2023-44487) Vespa Blog
HCSEC-2023-32 - Vault, Consul, and Boundary Affected By HTTP/2 “Rapid Reset” Denial of Service Vulnerability (CVE-2023-44487) - SecurityWeek
[SECURITY] Fedora 38 Update: mod_http2-2.0.25-1.fc38 - package-announce - Fedora Mailing-Lists
DSA-5558
net/http, x/net/http2: rapid stream resets can cause excessive work (CVE-2023-39325) · Issue #63417 · golang/go · GitHub

Release nhttp2 v1.57.0 · nhttp2/nhttp2 · GitHub
CVE-2023-44487: HTTP/2 Rapid Reset Attack · Issue #1872 · alibaba/tengine · GitHub
io.netty:netty-codec-http2 vulnerable to HTTP/2 Rapid Reset Attack · GHSA-xpw8-rcwv-8f8p · GitHub Advisory Database · GitHub
Add an HTTP/2 related rate limiting by maskit · Pull Request #10564 · apache/trafficserver · GitHub
Handling of CVE-2023-44487 / HTTP2 Rapid Reset · Issue #3996 · varnishcache/varnish-cache · GitHub
[SECURITY] Fedora 37 Update: folly-2023.10.16.00-1.fc37 - package-announce - Fedora Mailing-Lists
Apache Tomcat® - Apache Tomcat 10 vulnerabilities
Resets, Leaks, DDoS and the Tale of a Hidden CVE - Edgio
CVE-2023-44487 Ubuntu
cve-details
[SECURITY] Fedora 38 Update: mod_http2-2.0.25-1.fc38 - package-announce - Fedora Mailing-Lists
Go: Multiple Vulnerabilities (GLSA 202311-09) — Gentoo security
[SECURITY] Fedora 37 Update: golang-1.20.10-3.fc37 - package-announce - Fedora Mailing-Lists
swift-nio-http2 vulnerable to HTTP/2 Stream Cancellation Attack · CVE-2023-44487 · GitHub Advisory Database · GitHub
HTTP/2 Rapid Reset : CVE-2023-44487 · Issue #5877 · caddyserver/caddy · GitHub
[SECURITY] Fedora 38 Update: nhttp2-1.52.0-2.fc38 - package-announce - Fedora Mailing-Lists
Re-sync with internal repository following CVE-2023-44487 by facebook-github-bot · Pull Request #466 · facebook/proxygen · GitHub
Microsoft Response to Distributed Denial of Service (DDoS) Attacks against HTTP/2 MSRC Blog Microsoft Security Response Center
HTTP2 Rapid Reset - CVE-2023-44487 · Kong/kong · Discussion #11741 · GitHub
HTTP/2 Rapid Reset Vulnerability, CVE-2023-44487 CISA
[SECURITY] Fedora 38 Update: nodejs18-18.18.2-1.fc38 - package-announce - Fedora Mailing-Lists
Debian -- Security Information -- DSA-5522-1 tomcat9
[SECURITY] Fedora 37 Update: trafficserver-9.2.3-1.fc37 - package-announce - Fedora Mailing-Lists
Rework session management by tatsuhito-t · Pull Request #1961 · nhttp2/nhttp2 · GitHub
HTTP/2 Rapid Reset Attack Impacting NGINX Products - NGINX
CVE-2023-44487 Impact of Rapid Reset and HTTP/2 DoS Vulnerabilities (CVE-2023-44487, CVE-2023-35945)
[SECURITY] Fedora 37 Update: nodejs20-20.8.1-1.fc37 - package-announce - Fedora Mailing-Lists
ports - FreeBSD ports tree
[SECURITY] Fedora 37 Update: nhttp2-1.51.0-2.fc37 - package-announce - Fedora Mailing-Lists
CVE-2023-44487 issue/fix? · Issue #930 · openresty/openresty · GitHub
Prague side meeting: HTTP/2 concurrency and request cancellation (CVE-2023-44487) from Mark Nottingham on 2023-10-10 (ietf-http-wg@v
[SECURITY] Fedora 39 Update: trafficserver-9.2.3-1.fc39 - package-announce - Fedora Mailing-Lists
Google Cloud mitigated largest DDoS attack, peaking above 398 million rps Google Cloud Blog
[SECURITY] Fedora 39 Update: nodejs20-20.8.1-1.fc39 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 39 Update: mvfst-2023.10.16.00-1.fc39 - package-announce - Fedora Mailing-Lists

oss-security - Vulnerability in Jenkins
Swift-nio-http2 security update: CVE-2023-44487 HTTP/2 DOS - SwiftNIO - Swift Forums
[SECURITY] [DLA 3621-1] nghttp2 security update
Fix for nginx and golang for CVE-2023-44487 by ddstreetmicrosoft · Pull Request #6381 · microsoft/CBL-Mariner · GitHub
oss-security - Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
HAProxy is not affected by the HTTP/2 Rapid Reset Attack (CVE-2023-44487)
[SECURITY] Fedora 37 Update: nghttp2-1.51.0-2.fc37 - package-announce - Fedora Mailing-Lists
Debian -- Security Information -- DSA-5549-1 trafficserver
Using HTTP/3 Stream Limits in HTTP/2
oss-security - Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations
[SECURITY] Fedora 38 Update: golang-1.20.10-2.fc38 - package-announce - Fedora Mailing-Lists
Security Update Guide - Microsoft Security Response Center
[SECURITY] Fedora 39 Update: mvfst-2023.10.16.00-1.fc39 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 39 Update: nghttp2-1.55.1-4.fc39 - package-announce - Fedora Mailing-Lists
Release v2.7.5 · caddyserver/caddy · GitHub
CVE-2023-44487: Distributed Denial of Service (DDoS) Attacks against HTTP/2 · Issue #3947 · Azure/AKS · GitHub
GitHub - micrictor/http2-rst-stream
1216123 – (CVE-2023-44487) VUL-0: CVE-2023-44487: TRACKER-BUG: HTTP/2 Rapid Reset Attack
[SECURITY] Fedora 39 Update: golang-1.21.3-1.fc39 - package-announce - Fedora Mailing-Lists
The novel HTTP/2 'Rapid Reset' DDoS attack Hacker News
[SECURITY] [DLA 3645-1] trafficserver security update
HTTP/2 "Rapid Reset" DDoS Attack Disclosed By Google, Cloudflare & AWS - Phoronix
HTTP/2 Zero-Day Vulnerability Results in Record-Breaking DDoS Attacks
deps: update nghttp2 to 1.57.0 by jasnell · Pull Request #50121 · nodejs/node · GitHub
github.com/arkrwn/PoC/tree/main/CVE-2023-44487
[SECURITY] Fedora 39 Update: mod_http2-2.0.25-1.fc39 - package-announce - Fedora Mailing-Lists
[Announcement] CVE-2023-44487 (HTTP/2 Rapid Reset Attack) does not affect `rpxy` · Issue #97 · junkurihara/rust-rpxy · GitHub
4988 – HTTP/2 Rapid Reset : CVE-2023-44487
[SECURITY] Fedora 39 Update: nodejs18-18.18.2-1.fc39 - package-announce - Fedora Mailing-Lists
server: prohibit more than MaxConcurrentStreams handlers from running at once by dfawley · Pull Request #6703 · grpc/grpc-go · GitHub
HTTP/2 Zero-Day Vulnerability Results in Record-Breaking DDoS Attacks Hacker News
[SECURITY] Fedora 37 Update: trafficserver-9.2.3-1.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] [DLA 3617-1] tomcat9 security update
github.com/nghttp2/nghttp2 has HTTP/2 Rapid Reset · GHSA-vx74-f528-fxqg · GitHub Advisory Database · GitHub
[SECURITY] Fedora 39 Update: trafficserver-9.2.3-1.fc39 - package-announce - Fedora Mailing-Lists
CVE-2023-44487 (High) detected in multiple libraries · Issue #3474 · opensearch-project/data-prepper · GitHub

CVE-2023-44487 (High) detected in multiple libraries - Issue #7474 · opensearch-project/data-prepper · GitHub

Debian -- Security Information -- DSA-5540-1 jetty9

hyper HTTP/2 Rapid Reset Attack: Unaffected - seanmonstar

oss-security - Re: CVE-2023-44487: HTTP/2 Rapid Reset attack against many implementations

oss-security - CVE-2023-45802: Apache HTTP Server: HTTP/2 stream memory not reclaimed right away on RST

Merge pull request from GHSA-xpw8-rcwv-8f8p · netty/netty@58f75f6 · GitHub

Netlify Successfully Mitigates CVE-2023-44487

Internet-Wide Zero-Day Bug Fuels Largest-Ever DDoS Event

Rapid Reset HTTP/2 Vulnerability * LiteSpeed Blog

Does this recent http2 CVE affect this package? · Issue #93 · kazu-yamamoto/http2 · GitHub

lists.apache.org/thread/5py8h42mxfsn8l1wy6o41xwshjlsd87q

Istio / ISTIO-SECURITY-2023-004

[SECURITY] Fedora 38 Update: nodejs20-20.8.1-1.fc38 - package-announce - Fedora Mailing-Lists

ver bump up · kazu-yamamoto/http2@f61d41a · GitHub

HTTP/2 'Rapid Reset' zero-day exploited in biggest DDoS yet • The Register

[SECURITY] Fedora 38 Update: golang-1.20.10-2.fc38 - package-announce - Fedora Mailing-Lists

HAProxy is not affected by the HTTP/2 Rapid Reset Attack | Hacker News

CVE-2023-44487 · Issue #4323 · akka/akka-http · GitHub

HTTP/2 Rapid Reset Vulnerability Highlights Need for Rapid Response - Open Source Security Foundation

help request: What's the action for CVE-2023-44487 ? · Issue #10320 · apache/apisix · GitHub

github.com/apache/tomcat/tree/main/java/org/apache/coyote/http2

HTTP/2 Rapid Reset · Advisory · h2o/h2o · GitHub

github.com/dotnet/core/blob/e4613450ea0da7fd2fc6b61dfb2c1c1dec1ce9ec/rel...

[SECURITY] Fedora 39 Update: mod_http2-2.0.25-1.fc39 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 37 Update: mod_http2-2.0.25-1.fc37 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

150732 Apache Tomcat Multiple Vulnerabilities (CVE-2023-42795, CVE-2023-44487, CVE-2023-45648)

160986 Oracle Enterprise Linux Security Update for nginx:1.22 (ELSA-2023-5713)

160988 Oracle Enterprise Linux Security Update for nginx:1.20 (ELSA-2023-5712)

160990 Oracle Enterprise Linux Security Update for nginx (ELSA-2023-5711)
160992 Oracle Enterprise Linux Security Update for dotnet6.0 (ELSA-2023-5708)
160993 Oracle Enterprise Linux Security Update for dotnet6.0 (ELSA-2023-5710)
160995 Oracle Enterprise Linux Security Update for .net 7.0 (ELSA-2023-5749)
160996 Oracle Enterprise Linux Security Update for go-toolset:ol8 (ELSA-2023-5721)
160998 Oracle Enterprise Linux Security Update for go-toolset and golang (ELSA-2023-5738)
161002 Oracle Enterprise Linux Security Update for dotnet7.0 (ELSA-2023-5709)
161003 Oracle Enterprise Linux Security Update for nghttp2 (ELSA-2023-5837)
161004 Oracle Enterprise Linux Security Update for nghttp2 (ELSA-2023-5838)
161006 Oracle Enterprise Linux Security Update for nodejs (ELSA-2023-5765)
161007 Oracle Enterprise Linux Security Update for 18 (ELSA-2023-5849)
161009 Oracle Enterprise Linux Security Update for grafana (ELSA-2023-5867)
161010 Oracle Enterprise Linux Security Update for nodejs:18 (ELSA-2023-5869)
161011 Oracle Enterprise Linux Security Update for grafana (ELSA-2023-5863)
161012 Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2023-5850)
161013 Oracle Enterprise Linux Security Update for tomcat (ELSA-2023-5929)
161017 Oracle Enterprise Linux Security Update for varnish (ELSA-2023-5989)
161018 Oracle Enterprise Linux Security Update for varnish (ELSA-2023-5924)
161021 Oracle Enterprise Linux Security Update for tomcat (ELSA-2023-5928)
161025 Oracle Enterprise Linux Security Update for nginx:1.22 (ELSA-2023-6120)
161071 Oracle Enterprise Linux Security Update for nghttp2 (ELSA-2023-6746)
161192 Oracle Enterprise Linux Security Update for nodejs:20 (ELSA-2023-7205)
161216 Oracle Enterprise Linux Security Update for common (ELSA-2023-13029)
161217 Oracle Enterprise Linux Security Update for common (ELSA-2023-13028)
161254 Oracle Enterprise Linux Security Update for common (ELSA-2023-13053)
161255 Oracle Enterprise Linux Security Update for common (ELSA-2023-13054)
161431 Oracle Enterprise Linux Security Update for nodejs:16 (ELSA-2024-1444)
199823 Ubuntu Security Notification for .NET Vulnerability (USN-6427-1)
199905 Ubuntu Security Notification for .NET Vulnerabilities (USN-6438-1)

[199909](#) Ubuntu Security Notification for .NET Vulnerabilities (USN-6400-1)

[199910](#) Ubuntu Security Notification for .NET Vulnerability (USN-6427-2)

[199941](#) Ubuntu Security Notification for nghttp2 Vulnerability (USN-6505-1)

[200040](#) Ubuntu Security Notification for Go Vulnerabilities (USN-6574-1)

[20399](#) Oracle Database 19c Critical OJVM Patch Update - January 2024

[20400](#) Oracle Database 19c Critical Patch Update - January 2024

[20401](#) Oracle Database 21c Critical Patch Update - January 2024

[242166](#) Red Hat Update for nginx (RHSA-2023:5714)

[242167](#) Red Hat Update for rh-dotnet60-dotnet security (RHSA-2023:5705)

[242168](#) Red Hat Update for dotnet6.0 (RHSA-2023:5706)

[242169](#) Red Hat Update for nginx:1.20 (RHSA-2023:5715)

[242170](#) Red Hat Update for dotnet6.0 (RHSA-2023:5710)

[242171](#) Red Hat Update for dotnet6.0 (RHSA-2023:5708)

[242172](#) Red Hat Update for dotnet6.0 (RHSA-2023:5707)

[242173](#) Red Hat Update for go-toolset:rhel8 (RHSA-2023:5721)

[242174](#) Red Hat Update for rh-nginx120-nginx (RHSA-2023:5720)

[242175](#) Red Hat Update for .net 7.0 (RHSA-2023:5749)

[242176](#) Red Hat Update for go-toolset and golang (RHSA-2023:5738)

[242177](#) Red Hat Update for nghttp2 (RHSA-2023:5769)

[242178](#) Red Hat Update for nghttp2 (RHSA-2023:5768)

[242181](#) Red Hat Update for nodejs (RHSA-2023:5764)

[242182](#) Red Hat Update for nodejs (RHSA-2023:5765)

[242184](#) Red Hat Update for nghttp2 (RHSA-2023:5766)

[242189](#) Red Hat Update for nodejs:16 (RHSA-2023:5803)

[242193](#) Red Hat Update for rhc-worker-script enhancement and (RHSA-2023:5835)

[242194](#) Red Hat Update for rh-nodejs14 (RHSA-2023:5840)

[242195](#) Red Hat Update for nghttp2 (RHSA-2023:5838)

[242196](#) Red Hat Update for httpd24-httpd (RHSA-2023:5841)

[242197](#) Red Hat Update for nghttp2 (RHSA-2023:5837)

242198 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:5679)
242206 Red Hat Update for nodejs:16 (RHSA-2023:5850)
242208 Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:5717)
242212 Red Hat Update for grafana (RHSA-2023:5866)
242214 Red Hat Update for grafana (RHSA-2023:5864)
242219 Red Hat Update for grafana (RHSA-2023:5863)
242222 Red Hat Update for JBoss Enterprise Application Platform 7.4 (RHSA-2023:5920)
242224 Red Hat Update for varnish (RHSA-2023:5924)
242225 Red Hat Update for varnish (RHSA-2023:5930)
242226 Red Hat Update for tomcat (RHSA-2023:5928)
242228 Red Hat Update for OpenStack Platform 17.1.1 (RHSA-2023:5969)
242229 Red Hat Update for Satellite 6.11.5.6 (RHSA-2023:5980)
242230 Red Hat Update for Satellite 6.12.5.2 (RHSA-2023:5979)
242231 Red Hat Update for varnish (RHSA-2023:5989)
242234 Red Hat Update for varnish:6 (RHSA-2023:6020)
242237 Red Hat Update for varnish:6 (RHSA-2023:6023)
242238 Red Hat Update for varnish:6 (RHSA-2023:6022)
242239 Red Hat Update for varnish:6 (RHSA-2023:6021)
242241 Red Hat Update for toolbox (RHSA-2023:6057)
242244 Red Hat Update for toolbox (RHSA-2023:6077)
242245 Red Hat Update for nginx:1.22 (RHSA-2023:6120)
242246 Red Hat Update for JBoss Core Services (RHSA-2023:6105)
242307 Red Hat Update for nghttp2 (RHSA-2023:6746)
242347 Red Hat Update for Satellite 6.14 (RHSA-2023:6818)
242351 Red Hat Update for nginx:1.20 (RHSA-2023:5712)
242357 Red Hat Update for OpenStack Platform 17.1.1 (RHSA-2023:5970)
242362 Red Hat Update for grafana (RHSA-2023:5867)
242363 Red Hat Update for Satellite 6.13.5 (RHSA-2023:5931)

[242365](#) Red Hat Update for OpenStack Platform 16.2.5 (RHSA-2023:5964)

[242367](#) Red Hat Update for nghttp2 (RHSA-2023:5770)

[242370](#) Red Hat Update for dotnet7.0 (RHSA-2023:5709)

[242373](#) Red Hat Update for nginx (RHSA-2023:5711)

[242374](#) Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:5009)

[242376](#) Red Hat Update for nodejs:18 (RHSA-2023:5849)

[242378](#) Red Hat Update for OpenStack Platform 16.1.9 (RHSA-2023:5967)

[242381](#) Red Hat Update for OpenStack Platform 16.2.5 (RHSA-2023:5965)

[242385](#) Red Hat Update for nodejs:18 (RHSA-2023:5869)

[242387](#) Red Hat Update for nginx:1.22 (RHSA-2023:5713)

[242391](#) Red Hat Update for tomcat (RHSA-2023:5929)

[242394](#) Red Hat Update for nghttp2 (RHSA-2023:5767)

[242401](#) Red Hat Update for grafana (RHSA-2023:5865)

[242429](#) Red Hat Update for nodejs:20 (RHSA-2023:7205)

[242464](#) Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:6840)

[242465](#) Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:6839)

[242479](#) Red Hat Update for rh-varnish6-varnish (RHSA-2023:7334)

[242493](#) Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:7325)

[242533](#) Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:7481)

[242542](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 9 (RHSA-2023:7639)

[242543](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 8 (RHSA-2023:7638)

[242551](#) Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:7610)

[242565](#) Red Hat Update for JBoss Enterprise Application Platform 7.4.1 on RHEL 7 (RHSA-2023:7637)

[243104](#) Red Hat Update for nodejs:16 (RHSA-2024:1444)

[284629](#) Fedora Security Update for nghttp2 (FEDORA-2023-ed2642fd58)

[284641](#) Fedora Security Update for trafficserver (FEDORA-2023-5ff7bf1dd8)

[284643](#) Fedora Security Update for trafficserver (FEDORA-2023-54fadada12)

[284656](#) Fedora Security Update for mod_http2 (FEDORA-2023-0259c3f26f)

[284658](#) Fedora Security Update for cachelib (FEDORA-2023-2a9214af5f)

284659 Fedora Security Update for cachelib (FEDORA-2023-17efd3f2cd)
284660 Fedora Security Update for nodejs18 (FEDORA-2023-d5030c983c)
284672 Fedora Security Update for nodejs20 (FEDORA-2023-f66fc0f62a)
284673 Fedora Security Update for nodejs20 (FEDORA-2023-4d2fd884ea)
284674 Fedora Security Update for nodejs18 (FEDORA-2023-e9c04d81c1)
284683 Fedora Security Update for nhttp2 (FEDORA-2023-b2c50535cb)
284688 Fedora Security Update for golang (FEDORA-2023-fe53e13b5b)
284689 Fedora Security Update for golang (FEDORA-2023-4bf641255e)
284710 Fedora Security Update for mod_http2 (FEDORA-2023-c0c6a91330)
285180 Fedora Security Update for mod_http2 (FEDORA-2023-492b7be466)
285182 Fedora Security Update for golang (FEDORA-2023-822aab0a5a)
285184 Fedora Security Update for cachelib (FEDORA-2023-7934802344)
285187 Fedora Security Update for nodejs20 (FEDORA-2023-7b52921cae)
285188 Fedora Security Update for nodejs18 (FEDORA-2023-dbe64661af)
285199 Fedora Security Update for nhttp2 (FEDORA-2023-3f70b8d406)
285203 Fedora Security Update for trafficserver (FEDORA-2023-1caffb88af)
296105 Oracle Solaris 11.4 Support Repository Update (SRU) 63.157.1 Missing (CPUOCT2023)
296106 Oracle Solaris 11.4 Support Repository Update (SRU) 64.157.2 Missing (CPUOCT2023)
296108 Oracle Solaris 11.4 Support Repository Update (SRU) 66.164.1 Missing (CPUJAN2024)
317402 Cisco Secure Web Appliance HTTP/2 Rapid Reset Attack Vulnerability (CSCwh88595)
356400 Amazon Linux Security Advisory for nhttp2 : ALAS2-2023-2312
356411 Amazon Linux Security Advisory for golang : ALAS2-2023-2313
356446 Amazon Linux Security Advisory for nginx : ALAS-2023-1870
356453 Amazon Linux Security Advisory for nhttp2 : ALAS-2023-1869
356455 Amazon Linux Security Advisory for golang : ALAS-2023-1871
356456 Amazon Linux Security Advisory for tomcat8 : ALAS-2023-1868
356513 Amazon Linux Security Advisory for golang : ALAS2023-2023-394
356520 Amazon Linux Security Advisory for tomcat9 : ALAS2023-2023-390

356523 Amazon Linux Security Advisory for nginx : ALAS2023-2023-393
356526 Amazon Linux Security Advisory for nodejs : ALAS2023-2023-391
356540 Amazon Linux Security Advisory for nhttp2 : ALAS2023-2023-392
356541 Amazon Linux Security Advisory for dotnet6.0 : ALAS2023-2023-389
356556 Amazon Linux Security Advisory for tomcat : ALAS2TOMCAT8.5-2023-016
356581 Amazon Linux Security Advisory for tomcat : ALAS2TOMCAT9-2023-010
356587 Amazon Linux Security Advisory for nginx : ALAS2NGINX1-2023-006
356597 Amazon Linux Security Advisory for ecs-service-connect-agent : ALAS2ECS-2023-016
356624 Amazon Linux Security Advisory for ecs-service-connect-agent : ALAS2023-2023-420
378951 Node.js Multiple Security Vulnerabilities (October 13, 2023 Security Release)
378964 Alibaba Cloud Linux Security Update for grafana (ALINUX3-SA-2023:0131)
379045 Alibaba Cloud Linux Security Update for varnish (ALINUX3-SA-2023:0137)
379047 Alibaba Cloud Linux Security Update for nhttp2 (ALINUX3-SA-2023:0132)
379267 Oracle Coherence January 2024 Critical Patch Update (CPUJAN2024)
379437 Alibaba Cloud Linux Security Update for nginx:1.20 (ALINUX3-SA-2024:0016)
379452 IBM Cognos Analytics Multiple Vulnerabilities (7123154)
379516 IBM Sterling Secure Proxy Multiple Vulnerabilities (7142038)
379590 Gitlab Multiple Vulnerabilities (prior to gitlab- 16.5.1, 16.4.2, 16.3.6)
379646 Alibaba Cloud Linux Security Update for go-toolset:rhel8 (ALINUX3-SA-2024:0033)
44173 FortiOS Rapid Reset HTTP/2 Vulnerability (FG-IR-23-397)
503377 Alpine Linux Security Update for nhttp2
503378 Alpine Linux Security Update for nhttp2
503380 Alpine Linux Security Update for dotnet6-build
503381 Alpine Linux Security Update for dotnet6-runtime
503382 Alpine Linux Security Update for dotnet7-build
503383 Alpine Linux Security Update for dotnet7-runtime
503385 Alpine Linux Security Update for h2o
503386 Alpine Linux Security Update for go
503387 Alpine Linux Security Update for nhttp2

503390 Alpine Linux Security Update for jetty-runner
503391 Alpine Linux Security Update for nginx
503393 Alpine Linux Security Update for nginx
503419 Alpine Linux Security Update for nginx
503440 Alpine Linux Security Update for dotnet6-build
503441 Alpine Linux Security Update for dotnet6-runtime
503442 Alpine Linux Security Update for dotnet7-build
503443 Alpine Linux Security Update for dotnet7-runtime
503444 Alpine Linux Security Update for dotnet7-runtime
503468 Alpine Linux Security Update for lighttpd
503469 Alpine Linux Security Update for nghttp2
503629 Alpine Linux Security Update for varnish
505898 Alpine Linux Security Update for nghttp2
505899 Alpine Linux Security Update for nginx
505950 Alpine Linux Security Update for varnish
506007 Alpine Linux Security Update for dotnet6-build
506008 Alpine Linux Security Update for dotnet6-build
506015 Alpine Linux Security Update for dotnet6-runtime
506016 Alpine Linux Security Update for dotnet6-runtime
506023 Alpine Linux Security Update for dotnet7-build
506024 Alpine Linux Security Update for dotnet7-build
506028 Alpine Linux Security Update for dotnet7-runtime
506029 Alpine Linux Security Update for dotnet7-runtime
506088 Alpine Linux Security Update for go
506098 Alpine Linux Security Update for h2o
506101 Alpine Linux Security Update for jetty-runner
506124 Alpine Linux Security Update for netdata
510683 Alpine Linux Security Update for openjdk21

510805 Alpine Linux Security Update for varnish
6000246 Debian Security Update for tomcat9 (DSA 5522-1)
6000247 Debian Security Update for tomcat10 (DSA 5521-1)
6000251 Debian Security Update for tomcat9 (DLA 3617-2)
6000257 Debian Security Update for tomcat9 (DLA 3617-1)
6000263 Debian Security Update for h2o (DLA 3638-1)
6000267 Debian Security Update for jetty9 (DLA 3641-1)
6000268 Debian Security Update for trafficserver (DLA 3645-1)
6000281 Debian Security Update for nhttp2 (DLA 3621-1)
6000299 Debian Security Update for jetty9 (DSA 5540-1)
6000301 Debian Security Update for tomcat9 (DSA 5522-3)
6000303 Debian Security Update for tomcat9 (DSA 5522-2)
6000312 Debian Security Update for trafficserver (DSA 5549-1)
6000331 Debian Security Update for netty (DSA 5558-1)
6000332 Debian Security Update for netty (DLA 3656-1)
6000368 Debian Security Update for nhttp2 (DSA 5570-1)
673322 EulerOS Security Update for nhttp2 (EulerOS-SA-2024-1092)
673404 EulerOS Security Update for nhttp2 (EulerOS-SA-2024-1068)
673464 EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3282)
673519 EulerOS Security Update for golang (EulerOS-SA-2023-3270)
673612 EulerOS Security Update for golang (EulerOS-SA-2024-1082)
673636 EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3346)
673762 EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3254)
673850 EulerOS Security Update for golang (EulerOS-SA-2024-1140)
673892 EulerOS Security Update for nginx (EulerOS-SA-2024-1154)
673979 EulerOS Security Update for golang (EulerOS-SA-2023-3299)
673981 EulerOS Security Update for golang (EulerOS-SA-2024-1058)
673988 EulerOS Security Update for golang (EulerOS-SA-2023-3331)
674095 EulerOS Security Update for nhttp2 (EulerOS-SA-2023-3314)

671000 EulerOS Security Update for nginx (EulerOS-SA-2023-3217)
674107 EulerOS Security Update for golang (EulerOS-SA-2023-3242)
691321 Free Berkeley Software Distribution (FreeBSD) Security Update for h2o (bf545001-b96d-42e4-9d2e-60fdee204a43)
691327 Free Berkeley Software Distribution (FreeBSD) Security Update for traefik (7a1b2624-6a89-11ee-af06-5404a68ad561)
691330 Free Berkeley Software Distribution (FreeBSD) Security Update for jenkins (1ee26d45-6ddb-11ee-9898-00e081b7aa2d)
691368 Free Berkeley Software Distribution (FreeBSD) Security Update for varnish (f25a34b1-910d-11ee-a1a2-641c67a117d8)
710791 Gentoo Linux Go Multiple Vulnerabilities (GLSA 202311-09)
730934 Apache Tomcat Denial of Service Vulnerability (CVE-2023-42794)
730935 Apache Tomcat Information Disclosure Vulnerability (CVE-2023-42795)
730936 Apache Tomcat Denial of Service Vulnerability (CVE-2023-42794)
730937 Apache Tomcat Multiple Vulnerabilities
730958 Jenkins HTTP/2 Denial of Service (DoS) Vulnerability (Jenkins Security Advisory 2023-10-18)
730977 Atlassian Confluence Data Center and Server Denial of Service (DoS) Vulnerability (CONFSERVER-93163)
731034 Cisco Prime Infrastructure Distributed Denial of Service (DDoS) Vulnerability (cisco-sa-http2-reset-d8Kf32vZ)
755088 SUSE Enterprise Linux Security Update for go1.21 (SUSE-SU-2023:4069-1)
755089 SUSE Enterprise Linux Security Update for go1.20 (SUSE-SU-2023:4068-1)
755117 SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2023:4129-1)
755122 SUSE Enterprise Linux Security Update for nodejs18 (SUSE-SU-2023:4133-1)
755131 SUSE Enterprise Linux Security Update for nodejs18 (SUSE-SU-2023:4155-1)
755139 SUSE Enterprise Linux Security Update for netty, netty-tcnative (SUSE-SU-2023:4163-1)
755155 SUSE Enterprise Linux Security Update for nghttp2 (SUSE-SU-2023:4200-1)
755156 SUSE Enterprise Linux Security Update for nghttp2 (SUSE-SU-2023:4199-1)
755165 SUSE Enterprise Linux Security Update for jetty-minimal (SUSE-SU-2023:4210-1)
755167 SUSE Enterprise Linux Security Update for nodejs18 (SUSE-SU-2023:4207-1)
755201 SUSE Enterprise Linux Security Update for nodejs10 (SUSE-SU-2023:4295-1)
755230 SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2023:4374-1)
755231 SUSE Enterprise Linux Security Update for nodejs12 (SUSE-SU-2023:4373-1)
755272 SUSE Enterprise Linux Security Update for go1.20-openssl (SUSE-SU-2023:4472-1)
755275 SUSE Enterprise Linux Security Update for go1.21-openssl (SUSE-SU-2023:4469-1)

755292 SUSE Enterprise Linux Security Update for nhttp2 (SUSE-SU-2023:4492-1)
755902 SUSE Enterprise Linux Security Update for kubevirt, virt-api-container, virt-controller-container, virt-exportproxy-container, virt-exportserver-container, virt-handler-container, virt-launcher-container, virt-libguestfs-t (SUSE-SU-2023:4624-1)
770209 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:5679)
770210 Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:5717)
770213 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:5009)
770214 Red Hat OpenShift Container Platform 4.14 Security Update (RHSA-2023:6840)
770215 Red Hat OpenShift Container Platform 4.13 Security Update (RHSA-2023:7325)
770217 Red Hat OpenShift Container Platform 4.11 Security Update (RHSA-2023:7481)
770219 Red Hat OpenShift Container Platform 4.12 Security Update (RHSA-2023:7610)
907423 Common Base Linux Mariner (CBL-Mariner) Security Update for nginx (31333)
907426 Common Base Linux Mariner (CBL-Mariner) Security Update for cmake (31299-1)
907428 Common Base Linux Mariner (CBL-Mariner) Security Update for skopeo (31345-1)
907429 Common Base Linux Mariner (CBL-Mariner) Security Update for rook (31343-1)
907431 Common Base Linux Mariner (CBL-Mariner) Security Update for vitess (31348-1)
907432 Common Base Linux Mariner (CBL-Mariner) Security Update for prometheus (31341-1)
907433 Common Base Linux Mariner (CBL-Mariner) Security Update for prometheus-adapter (31342-1)
907434 Common Base Linux Mariner (CBL-Mariner) Security Update for kured (31319-1)
907435 Common Base Linux Mariner (CBL-Mariner) Security Update for flannel (31307-1)
907436 Common Base Linux Mariner (CBL-Mariner) Security Update for terraform (31347-1)
907437 Common Base Linux Mariner (CBL-Mariner) Security Update for cert-manager (31296-1)
907438 Common Base Linux Mariner (CBL-Mariner) Security Update for azcopy (31292-1)
907439 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (31325-1)
907440 Common Base Linux Mariner (CBL-Mariner) Security Update for kubevirt (31318-1)
907441 Common Base Linux Mariner (CBL-Mariner) Security Update for multus (31331-1)
907442 Common Base Linux Mariner (CBL-Mariner) Security Update for influxdb (31312-1)
907443 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-compose (31327-1)
907445 Common Base Linux Mariner (CBL-Mariner) Security Update for grpc (31520-1)
907446 Common Base Linux Mariner (CBL-Mariner) Security Update for kata-containers (31314-1)

907447	Common Base Linux Mariner (CBL-Mariner) Security Update for etcd (31306-1)
907448	Common Base Linux Mariner (CBL-Mariner) Security Update for containerized-data-importer (31300-1)
907449	Common Base Linux Mariner (CBL-Mariner) Security Update for kube-vip-cloud-provider (31317-1)
907451	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (31519-1)
907452	Common Base Linux Mariner (CBL-Mariner) Security Update for application-gateway-kubernetes-ingress (31291-1)
907453	Common Base Linux Mariner (CBL-Mariner) Security Update for nghttp2 (31332-1)
907454	Common Base Linux Mariner (CBL-Mariner) Security Update for kata-containers-cc (31315-1)
907456	Common Base Linux Mariner (CBL-Mariner) Security Update for keda (31316-1)
907457	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-cli (31326-1)
907458	Common Base Linux Mariner (CBL-Mariner) Security Update for nmi (31335-1)
907459	Common Base Linux Mariner (CBL-Mariner) Security Update for csi-driver-lvm (31305-1)
907462	Common Base Linux Mariner (CBL-Mariner) Security Update for cri-tools (31304-1)
907463	Common Base Linux Mariner (CBL-Mariner) Security Update for local-path-provisioner (31324-1)
907464	Common Base Linux Mariner (CBL-Mariner) Security Update for opa (31493-1)
907465	Common Base Linux Mariner (CBL-Mariner) Security Update for coredns (31301-1)
907467	Common Base Linux Mariner (CBL-Mariner) Security Update for packer (31340-1)
907469	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-containerd-cc (31491-1)
907470	Common Base Linux Mariner (CBL-Mariner) Security Update for jx (31313-1)
907472	Common Base Linux Mariner (CBL-Mariner) Security Update for node-problem-detector (31336-1)
907473	Common Base Linux Mariner (CBL-Mariner) Security Update for sriov-network-device-plugin (31346-1)
907474	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-engine (31329-1)
907475	Common Base Linux Mariner (CBL-Mariner) Security Update for cf-cli (31297-1)
907476	Common Base Linux Mariner (CBL-Mariner) Security Update for moby-containerd (31328-1)
907477	Common Base Linux Mariner (CBL-Mariner) Security Update for libcontainers-common (31323-1)
907478	Common Base Linux Mariner (CBL-Mariner) Security Update for telegraf (31498-1)
907480	Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs18 (31339-1)
907503	Common Base Linux Mariner (CBL-Mariner) Security Update for nginx (31333-1)
907513	Common Base Linux Mariner (CBL-Mariner) Security Update for golang (31519-2)
907500	Common Base Linux Mariner (CBL-Mariner) Security Update for etcd (31306-1)

907593 Common Base Linux Mariner (CBL-Mariner) Security Update for kubernetes (31693-1)
907598 Common Base Linux Mariner (CBL-Mariner) Security Update for nodejs18 (31339-2)
907792 Common Base Linux Mariner (CBL-Mariner) Security Update for coredns (31301-2)
907833 Common Base Linux Mariner (CBL-Mariner) Security Update for helm (33343-1)
907863 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (31519-3)
907895 Common Base Linux Mariner (CBL-Mariner) Security Update for local-path-provisioner (31324-2)
907900 Common Base Linux Mariner (CBL-Mariner) Security Update for packer (31340-2)
907902 Common Base Linux Mariner (CBL-Mariner) Security Update for azcopy (31292-2)
907903 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-buildx (31325-2)
907905 Common Base Linux Mariner (CBL-Mariner) Security Update for containerized-data-importer (31300-2)
907909 Common Base Linux Mariner (CBL-Mariner) Security Update for vitess (31348-2)
907910 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-containerd-cc (31491-2)
907913 Common Base Linux Mariner (CBL-Mariner) Security Update for kube-vip-cloud-provider (31317-2)
907919 Common Base Linux Mariner (CBL-Mariner) Security Update for kubevirt (31318-2)
907922 Common Base Linux Mariner (CBL-Mariner) Security Update for terraform (31347-2)
907923 Common Base Linux Mariner (CBL-Mariner) Security Update for moby-compose (31327-2)
907930 Common Base Linux Mariner (CBL-Mariner) Security Update for cf-cli (31297-2)
907931 Common Base Linux Mariner (CBL-Mariner) Security Update for application-gateway-kubernetes-ingress (31291-2)
907933 Common Base Linux Mariner (CBL-Mariner) Security Update for jx (31313-2)
907945 Common Base Linux Mariner (CBL-Mariner) Security Update for rook (31343-2)
907984 Common Base Linux Mariner (CBL-Mariner) Security Update for keda (31316-2)
908040 Common Base Linux Mariner (CBL-Mariner) Security Update for golang (37314-1)
92067 Microsoft HTTP/2 Protocol Distributed Denial of Service (DoS) Vulnerability
92070 Microsoft Azure Stack Hub Security Updates for October 2023
92072 Microsoft .NET Security Update for October 2023
941295 AlmaLinux Security Update for nginx:1.22 (ALSA-2023:5713)
941296 AlmaLinux Security Update for go-toolset:rhel8 (ALSA-2023:5721)
941297 AlmaLinux Security Update for dotnet7.0 (ALSA-2023:5709)
941298 AlmaLinux Security Update for go-toolset and golang (ALSA-2023:5738)

941299 AlmaLinux Security Update for nginx (ALSA-2023:5711)
941300 AlmaLinux Security Update for dotnet6.0 (ALSA-2023:5708)
941301 AlmaLinux Security Update for .NET (ALSA-2023:5749)
941302 AlmaLinux Security Update for nodejs (ALSA-2023:5765)
941304 AlmaLinux Security Update for nhttp2 (ALSA-2023:5837)
941305 AlmaLinux Security Update for nodejs:16 (ALSA-2023:5850)
941306 AlmaLinux Security Update for nodejs:18 (ALSA-2023:5869)
941308 AlmaLinux Security Update for grafana (ALSA-2023:5863)
941309 AlmaLinux Security Update for nodejs:18 (ALSA-2023:5849)
941310 AlmaLinux Security Update for grafana (ALSA-2023:5867)
941311 AlmaLinux Security Update for nhttp2 (ALSA-2023:5838)
941312 AlmaLinux Security Update for tomcat (ALSA-2023:5928)
941317 AlmaLinux Security Update for dotnet6.0 (ALSA-2023:5710)
941318 AlmaLinux Security Update for tomcat (ALSA-2023:5929)
941320 AlmaLinux Security Update for varnish (ALSA-2023:5924)
941326 AlmaLinux Security Update for nginx:1.20 (ALSA-2023:5712)
941328 AlmaLinux Security Update for varnish (ALSA-2023:5989)
941329 AlmaLinux Security Update for toolbox (ALSA-2023:6077)
941330 AlmaLinux Security Update for nginx:1.22 (ALSA-2023:6120)
941407 AlmaLinux Security Update for nhttp2 (ALSA-2023:6746)
941479 AlmaLinux Security Update for nodejs:20 (ALSA-2023:7205)
941626 AlmaLinux Security Update for nodejs:16 (ALSA-2024:1444)
961048 Rocky Linux Security Update for nhttp2 (RLSA-2023:5838)
961049 Rocky Linux Security Update for nodejs:16 (RLSA-2023:5850)
961050 Rocky Linux Security Update for tomcat (RLSA-2023:5928)
961053 Rocky Linux Security Update for nodejs (RLSA-2023:5765)
961055 Rocky Linux Security Update for varnish (RLSA-2023:5989)
961056 Rocky Linux Security Update for grafana (RLSA-2023:5863)

961058 Rocky Linux Security Update for go-toolset and golang (RLSA-2023:5738)
961059 Rocky Linux Security Update for varnish (RLSA-2023:5924)
961060 Rocky Linux Security Update for .NET (RLSA-2023:5749)
961061 Rocky Linux Security Update for dotnet6.0 (RLSA-2023:5708)
961063 Rocky Linux Security Update for go-toolset:rhel8 (RLSA-2023:5721)
961064 Rocky Linux Security Update for nginx:1.22 (RLSA-2023:6120)
961065 Rocky Linux Security Update for Satellite (RLSA-2023:6818)
961071 Rocky Linux Security Update for toolbox (RLSA-2023:6077)
961072 Rocky Linux Security Update for nghttp2 (RLSA-2023:6746)
961085 Rocky Linux Security Update for nodejs:20 (RLSA-2023:7205)
961141 Rocky Linux Security Update for nodejs:16 (RLSA-2024:1444)
995570 GO (Go) Security Update for golang.org/x/net (GHSA-qppj-fm5r-hxr3)
996444 Java (Maven) Security Update for golang.org/x/net (GHSA-qppj-fm5r-hxr3)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)