SCRUTEX · VULNERABILITY INTELLIGENCE

Vulnerability & Threat Intelligence Report

6 products · 30 CVEs mapped · 8 on CISA KEV · Generated 27 July 2026

EXECUTIVE SUMMARY

Portfolio exposure at a glance

This report covers 6 tracked products. It maps each to its live CVE exposure, marks which vulnerabilities sit on the CISA Known Exploited Vulnerabilities (KEV) catalog, and — where AI enrichment has run — names the threat actors tied to active exploitation.

PRODUCTS	CVES MAPPED	ON CISA KEV	EXPLOITED / ITW	THREAT ACTORS
6	30	8	8	6

Products ranked by urgency

PRODUCT	VENDOR / PLATFORM	CVES	KEV	URGENCY
Cisco C8300-1N1S-6T	Cisco · Cisco IOS XE	7	4	Critical
Cisco C8300-1N1S-4T2X	Cisco · Cisco IOS XE	7	4	Critical
Cisco Catalyst 9300	Cisco · Cisco IOS XE	8	4	Critical
Versa CSG2500	Versa Networks · Versa OS (VOS)	12	2	Critical
Versa CSG355	Versa Networks · Versa OS (VOS)	12	2	Critical
Juniper QFX5100	Juniper · Junos OS	7	1	High

CISCO · CATALYST 8300 EDGE / SD-WAN ROUTER

Cisco C8300-1N1S-6T

Critical. Same IOS XE exposure as the 4T2X SKU; Web UI zero-days apply, Smart Install does not.

Applicable CVEs (2)

CVE	SEVERITY	EPSS	KEV	EXPLOITS
CVE-2023-20198	Critical 10.0	100%	KEV	35 PoC
CVE-2023-20273	High 7.2	90%	KEV	1 PoC

Feature-conditional CVEs (5)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2025-20352	High 7.7	38%	KEV	SNMP stack overflow; affected with SNMP enabled (Operation Zero Disco).
CVE-2023-20109	Medium 6.6	2%	KEV	GET VPN RCE; the 8300 is the primary exposure. If GET VPN / GDOI configured.
CVE-2025-20154	High 8.6	0%	—	TWAMP DoS; if TWAMP configured.
CVE-2021-1529	High 7.8	0%	—	IOS XE SD-WAN command injection to root; Controller mode.
CVE-2023-20035	High 7.8	0%	—	IOS XE SD-WAN CLI command injection to root; Controller mode. [auto-ingest: MISS — NVD CPE is cisco:ios_xe_sd-wan, cisco:catalyst_8000v_edge, cisco:1100-4g\/6g_integrated_services_router, cisco:1100-4p_integrated_services_router]

Explicitly not applicable (1)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2018-0171	Critical 9.8	100%	KEV	Smart Install is a client-switch feature; the 8300 edge router does not run it. [auto-ingest: MISS — NVD CPE is cisco:ios]

CISCO · CATALYST 8300 EDGE / SD-WAN ROUTER

Cisco C8300-1N1S-4T2X

Critical. Web UI zero-days apply; Smart Install does NOT — the 8300 edge router does not run that client-switch feature.

Applicable CVEs (2)

CVE	SEVERITY	EPSS	KEV	EXPLOITS
CVE-2023-20198	Critical 10.0	100%	KEV	35 PoC
CVE-2023-20273	High 7.2	90%	KEV	1 PoC

Feature-conditional CVEs (5)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2025-20352	High 7.7	38%	KEV	SNMP stack overflow; affected with SNMP enabled (Operation Zero Disco).
CVE-2023-20109	Medium 6.6	2%	KEV	GET VPN RCE; the 8300 is the primary exposure. If GET VPN / GDOI configured.
CVE-2025-20154	High 8.6	0%	—	TWAMP DoS; if TWAMP configured.
CVE-2021-1529	High 7.8	0%	—	IOS XE SD-WAN command injection to root; Controller mode.
CVE-2023-20035	High 7.8	0%	—	IOS XE SD-WAN CLI command injection to root; Controller mode. [auto-ingest: MISS — NVD CPE is cisco:ios_xe_sd-wan, cisco:catalyst_8000v_edge, cisco:1100-4g\/6g_integrated_services_router, cisco:1100-4p_integrated_services_router]

Explicitly not applicable (1)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2018-0171	Critical 9.8	100%	KEV	Smart Install is a client-switch feature; the 8300 edge router does not run it. [auto-ingest: MISS — NVD CPE is cisco:ios]

CISCO · STACKABLE ACCESS/AGGREGATION SWITCH

Cisco Catalyst 9300

Critical. Web UI zero-days (CVE-2023-20198 + 20273, BadCandy) and Smart Install (CVE-2018-0171) both apply; Salt Typhoon activity.

Applicable CVEs (5)

CVE	SEVERITY	EPSS	KEV	EXPLOITS
CVE-2023-20198	Critical 10.0	100%	KEV	35 PoC
CVE-2018-0171	Critical 9.8	100%	KEV	1 PoC
CVE-2023-20273	High 7.2	90%	KEV	1 PoC
CVE-2025-20311	High 7.4	0%	—	
CVE-2023-20082	Medium 6.1	0%	—	

Feature-conditional CVEs (3)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2025-20352	High 7.7	38%	KEV	SNMP stack overflow; affected with SNMP enabled (Operation Zero Disco).
CVE-2025-20188	Critical 10.0	18%	—	WLC file upload; only with the embedded WLC + OOB AP image download.
CVE-2025-20154	High 8.6	0%	—	TWAMP DoS; if TWAMP configured.

Explicitly not applicable (2)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2024-20353	High 8.6	71%	KEV	Cisco ASA / FTD flaw — not a Catalyst IOS XE issue. [auto-ingest: MISS — NVD CPE is cisco:adaptive_security_appliance_software, cisco:firepower_threat_defense]
CVE-2024-20406	High 7.4	0%	—	Cisco IOS XR only — not IOS XE. [auto-ingest: MISS — NVD CPE is cisco:ios_xr]

VERSA NETWORKS · SD-WAN / SASE HUB GATEWAY

Versa CSG2500

High (via management plane). Protect the Director / Concerto tier and management ports and the CSG gateways are protected with it.

Applicable CVEs (3)

CVE	SEVERITY	EPSS	KEV	EXPLOITS
CVE-2018-16495	High 8.8	1%	—	
CVE-2018-16497	High 7.8	0%	—	
CVE-2018-16496	Medium 5.3	1%	—	

Feature-conditional CVEs (9)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2025-34026	High 7.5	83%	KEV	Concerto auth bypass, Actuator exposure; via Concerto.
CVE-2024-39717	High 7.2	4%	KEV	Versa Director web shell (VersaMem, Volt Typhoon); reached via the management plane.
CVE-2025-34027	Critical 10.0	37%	—	Concerto auth bypass to RCE; via the Concerto orchestrator. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2024-42450	Critical 10.0	1%	—	Director default Postgres config; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-34025	High 8.6	0%	—	Concerto Docker container escape; via Concerto. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-23171	High 7.2	0%	—	Director uCPE image-upload webshell; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-23172	High 7.2	1%	—	Director webhook SSRF to command exec; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2024-45229	Medium 6.6	1%	—	Director REST API token exposure; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-23168	Medium 6.3	0%	—	Director 2FA/OTP redirection; via management plane.

VERSA NETWORKS · SD-WAN / SASE BRANCH GATEWAY

Versa CSG355

High (via management plane). No CVE names the CSG355 hardware; exposure is inherited through a compromised Versa Director / Concerto.

Applicable CVEs (3)

CVE	SEVERITY	EPSS	KEV	EXPLOITS
CVE-2018-16495	High 8.8	1%	—	
CVE-2018-16497	High 7.8	0%	—	
CVE-2018-16496	Medium 5.3	1%	—	

Feature-conditional CVEs (9)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2025-34026	High 7.5	83%	KEV	Concerto auth bypass, Actuator exposure; via Concerto.
CVE-2024-39717	High 7.2	4%	KEV	Versa Director web shell (VersaMem, Volt Typhoon); reached via the management plane.
CVE-2025-34027	Critical 10.0	37%	—	Concerto auth bypass to RCE; via the Concerto orchestrator. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2024-42450	Critical 10.0	1%	—	Director default Postgres config; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-34025	High 8.6	0%	—	Concerto Docker container escape; via Concerto. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-23171	High 7.2	0%	—	Director uCPE image-upload webshell; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-23172	High 7.2	1%	—	Director webhook SSRF to command exec; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2024-45229	Medium 6.6	1%	—	Director REST API token exposure; via management plane. [auto-ingest: MISS — NVD has no CPE data yet]
CVE-2025-23168	Medium 6.3	0%	—	Director 2FA/OTP redirection; via management plane.

JUNIPER · DATA-CENTER TOP-OF-RACK / SPINE SWITCH

Juniper QFX5100

Medium-High. Platform-wide Junos kernel (CVE-2025-21590) and httpd (CVE-2024-47497) flaws apply; J-Web RCE chains are SRX/EX-only.

Applicable CVEs (2)

CVE	SEVERITY	EPSS	KEV	EXPLOITS
CVE-2025-21590	Medium 4.4	2%	KEV	
CVE-2024-47497	High 7.5	1%	—	

Feature-conditional CVEs (5)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2023-44191	High 7.5	1%	—	PFE VLAN DoS; QFX5000 Series — verify exact model line.
CVE-2024-39516	High 7.5	0%	—	rpd BGP DoS; if BGP traceoptions configured.
CVE-2024-39549	High 7.5	0%	—	rpd BGP DoS; if BGP is configured.
CVE-2025-21591	High 7.4	0%	—	jdhcpd DoS; affected when DHCP snooping is enabled.
CVE-2023-44183	Medium 6.5	0%	—	VxLAN PFE DoS; VxLAN deployments — verify.

Explicitly not applicable (4)

CVE	SEVERITY	EPSS	KEV	APPLICABILITY NOTE
CVE-2023-36844	Medium 5.3	91%	KEV	J-Web preAuth RCE chain — SRX/EX only. Not QFX5100 (on KEV, exploited).
CVE-2024-21591	Critical 9.8	18%	—	J-Web OOB write RCE — SRX/EX only. Not QFX5100.
CVE-2025-21599	High 7.5	1%	—	Junos OS Evolved only — QFX5100 runs classic Junos. [auto-ingest: MISS — NVD CPE is juniper:junos_os_evolved]
CVE-2025-21601	High 7.5	0%	—	Advisory lists QFX5120, not QFX5100.

Threat actors

Salt Typhoon Actor · China (state)

Living-off-the-land across telecom carriers; JumbledPath Go tool for packet capture and log erasure.

`CVE-2018-0171, CVE-2023-20198, CVE-2023-20273`

Static Tundra Actor · Russia (state)

Smart Install exploitation of unpatched/EoL Cisco devices for intelligence collection (~250k exposed 4786).

`CVE-2018-0171`

UNC3886 Actor · China (state)

Six TINYSHELL backdoor variants on Junos MX routers; Veriexec bypass via memory injection.

`CVE-2025-21590`

Volt Typhoon Actor · China (state)

VersaMem in-memory Java web shell hooks Director auth to steal credentials; access via port 4566.

`CVE-2024-39717`

BadCandy mass exploitation (unattributed) Campaign · Unknown (Oct 2023)

Chained the IOS XE Web UI zero-days to implant the BadCandy Lua web shell on 40,000+ devices.

`CVE-2023-20198, CVE-2023-20273`

J-Magic / cd00r Campaign · Unknown (Lumen)

In-memory magic-packet backdoor on enterprise Junos routers / VPN gateways; RSA-gated reverse shell. Not QFX.

Prioritised action plan

1. Patch now — known exploited (8)

On the CISA KEV catalog. Actively exploited and, for federal systems, bound by a remediation deadline.

CVE-2018-0171, CVE-2023-20198, CVE-2023-20273, CVE-2023-20109, CVE-2024-39717, CVE-2025-21590, CVE-2025-20352, CVE-2025-34026

2. High exploitation risk (2)

A public exploit exists or EPSS puts near-term exploitation above 10%. Prioritise after KEV.

CVE-2025-34027, CVE-2025-20188

3. Critical severity (1)

CVSS 9.0+ with no exploit signal yet — schedule promptly.

CVE-2024-42450

4. High severity (14)

CVSS 7.0–8.9. Fold into the regular patch cycle.

CVE-2018-16495, CVE-2025-20154, CVE-2025-34025, CVE-2023-20035, CVE-2021-1529, CVE-2018-16497, CVE-2024-47497, CVE-2024-39549, CVE-2024-39516, CVE-2023-44191, CVE-2025-20311, CVE-2025-21591, CVE-2025-23171, CVE-2025-23172

Sources & caveats

CVE base scores and descriptions: NVD (nvd.nist.gov).
KEV status and remediation due dates: CISA Known Exploited Vulnerabilities catalog.
Exploitation probability: FIRST.org EPSS.
Public exploit repositories: nomi-sec PoC-in-GitHub (unvetted; presence ≠ exploit quality).
Threat-actor and IOC intelligence is AI-researched with web search and carries source URLs; it is marked as such in the tool and should be verified before operational action.
Auto-mapped CVEs are matched by CPE and may include false positives — verify applicability.

Generated by Scrutex Vulnerability Intelligence on 27 July 2026. Re-verify KEV status and vendor fixed-versions before operational action.