

CVE-2023-20273

Cisco IOS XE Web UI Command Injection Vulnerability

CISA KEV since Oct 23, 2023

Actively exploited

Public exploit module (Metasploit)

A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.

EVRS 82/100 Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.930 99.83rd percentile · FIRST	CISA DEADLINE Oct 27, 2023 KEV since 2023 · listed over a year
--	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.930 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Verify that instances of Cisco IOS XE Web UI are in compliance with BOD 23-02 and apply mitigations per vendor instructions. For affected products (Cisco IOS XE Web UI exposed to the internet or to untrusted networks), follow vendor instructions to determine if a system may have been compromised and immediately report positive findings to CISA.

Basis: CISA KEV required action

Affected and fixed versions · 116 more affected products on the NVD record

ios xe	16.1.1	17.3.8a · 17.6.6a · 17.9.4a · NVD
	16.1.2	
	16.1.3	16.12.10a
	16.2.1	
	16.2.2	
	16.3.1a	
	16.3.2	
	16.3.3	
	16.3.4	
	16.3.5	
	16.3.5b	
	16.3.6	
	16.3.7	
	16.3.8	
	16.3.9	
	16.3.10	
	16.3.11	
	16.4.1	
	16.4.2	
	16.4.3	
	16.5.1	
	16.5.1a	
	16.5.1b	
	16.5.2	
	16.5.3	
	16.6.1	
	16.6.2	
	16.6.3	
	16.6.4	
	16.6.4a	
	16.6.5	
	16.6.5a	
	16.6.6	
	16.6.7	
	16.6.8	
	16.6.9	
	16.6.10	
	16.7.1	
	16.7.1a	
	16.7.1b	
	16.7.2	
	16.7.3	
	16.7.4	
	16.8.1	
	16.8.1a	
	16.8.1b	
	16.8.1c	
	16.8.1d	
	16.8.1e	
	16.8.1s	
	16.8.2	
	16.8.3	
	16.9.1	
	16.9.1a	
	16.9.1b	
	16.9.1s	
	16.9.2	
	16.9.3	
	16.9.3a	
	16.9.4	
	16.9.5	
	16.9.5f	
	16.9.6	

16.9.7
16.9.8
16.10.1
16.10.1a
16.10.1b
16.10.1c
16.10.1d
16.10.1e
16.10.1f
16.10.1g
16.10.1s
16.10.2
16.10.3
16.11.1
16.11.1a
16.11.1b
16.11.1s
16.11.2
16.12.1
16.12.1a
16.12.1c
16.12.1s
16.12.1t
16.12.1w
16.12.1x
16.12.1y
16.12.1z1
16.12.1z2
16.12.2
16.12.2a
16.12.2s
16.12.3
16.12.3a
16.12.3s
16.12.4
16.12.4a
16.12.5
16.12.5a
16.12.5b
16.12.6
16.12.6a
16.12.7
16.12.8
16.12.9
16.12.10
17.1.1
17.1.1a
17.1.1s
17.1.1t
17.1.3
17.2.1
17.2.1a
17.2.1r
17.2.1v
17.2.2
17.2.3
17.3.1
17.3.1a
17.3.1w
17.3.1x
17.3.1z
17.3.2
17.3.2a
17.3.3

17.3.4
 17.3.4a
 17.3.4b
 17.3.4c
 17.3.5
 17.3.5a
 17.3.5b
 17.3.6
 17.3.7
 17.3.8
 17.4.1
 17.4.1a
 17.4.1b
 17.4.2
 17.4.2a
 17.5.1
 17.5.1a
 17.5.1b
 17.5.1c
 17.6.1
 17.6.1a
 17.6.1w
 17.6.1x
 17.6.1y
 17.6.1z
 17.6.1z1
 17.6.2
 17.6.3
 17.6.3a
 17.6.4
 17.6.5
 17.6.6
 17.7.1
 17.7.1a
 17.7.1b
 17.7.2
 17.8.1
 17.8.1a
 17.9.1
 17.9.1a
 17.9.1w
 17.9.1x
 17.9.1x1
 17.9.1y
 17.9.1y1
 17.9.2
 17.9.2a
 17.9.3
 17.9.3a
 17.9.4
 17.10.1
 17.10.1a
 17.10.1b
 17.11.1
 17.11.1a
 17.11.99sw
 17.12.1
 17.12.1a
 ≥ 17.3 < 17.3.8a
 ≥ 17.6 < 17.6.6a
 ≥ 17.9 < 17.9.4a
 ≥ 16.12 < 16.12.10a

catalyst 3650

–

no fixed version listed

NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
catalyst 3650-12x48fd-e	–	no fixed version listed	NVD
catalyst 3650-12x48fd-l	–	no fixed version listed	NVD
catalyst 3650-12x48fd-s	–	no fixed version listed	NVD
catalyst 3650-12x48uq	–	no fixed version listed	NVD
catalyst 3650-12x48uq-e	–	no fixed version listed	NVD
catalyst 3650-12x48uq-l	–	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-xm3x-5hpf-5369

Additional guidance sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

NVD nvd.nist.gov/vuln/detail/CVE-2023-20273

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2023-24452

Current data evulnable.com/vulnerability-management/cve/CVE-2023-20273

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.