

CVE-2021-1497

Cisco HyperFlex HX Installer Virtual Machine Command Injection Vulnerability

Exigent CISA KEV since Nov 3, 2021 Actively exploited Public exploit module (Metasploit)

Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to perform command injection attacks against an affected device. For more information about these vulnerabilities, see the Details section of this advisory.

EVRS 87 / 100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.999 99.97th percentile · FIRST	CISA DEADLINE Nov 17, 2021 KEV since 2021 · 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	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified
CISA required action: Apply updates per vendor instructions.
 Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
hyperflex hx data platform	< 4.0\2e\) ≥ 4.5 < 4.5\2a\)	4.0\2e\) · 4.5\2a\)	NVD
hyperflex hx220c af m5	—	no fixed version listed	NVD
hyperflex hx220c all nvme m5	—	no fixed version listed	NVD
hyperflex hx220c edge m5	—	no fixed version listed	NVD
hyperflex hx220c m5	—	no fixed version listed	NVD
hyperflex hx240c	—	no fixed version listed	NVD
hyperflex hx240c af m5	—	no fixed version listed	NVD
hyperflex hx240c m5	—	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-2hv5-x25m-j674	Additional guidance	tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrKpR
NVD	nvd.nist.gov/vuln/detail/CVE-2021-1497	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-6964	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-1497

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