



CVE-2021-1498

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

Summary

CVE	CVE-2021-1498
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-06 13:15:00 UTC
Updated	2023-11-07 03:28:00 UTC
Description	Multiple vulnerabilities in the web-based management interface of Cisco HyperFlex HX could allow an unauthenticated, remote attacker to execute arbitrary code on the affected system. The vulnerability is due to a buffer overflow in the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. Successful exploitation could result in an attacker executing arbitrary code on the affected system. Cisco has released a software update to address this vulnerability. Users are advised to apply the update as soon as possible. (CWE-78)

Risk And Classification

EPSS: 0.942060000 probability, percentile 0.999240000 (date 2026-05-08)

CISA KEV: Listed on 2021-11-03; due 2021-11-17; ransomware use Unknown

Problem Types: CWE-78

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	HyperFlex HX
Name	Cisco HyperFlex HX Data Platform Command Injection Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-1498

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Hyperflex Hx220c Af M5	-	All	All	All
Hardware	Cisco	Hyperflex Hx220c All Nvme M5	-	All	All	All
Hardware	Cisco	Hyperflex Hx220c Edge M5	-	All	All	All
Hardware	Cisco	Hyperflex Hx220c M5	-	All	All	All
Hardware	Cisco	Hyperflex Hx240c	-	All	All	All
Hardware	Cisco	Hyperflex Hx240c Af M5	-	All	All	All
Hardware	Cisco	Hyperflex Hx240c M5	-	All	All	All
Operating System	Cisco	Hyperflex Hx Data Platform	All	All	All	All

Operating System	Cisco	Hyperflex Hx Data Platform	All	All	All	All
Operating System	Cisco	Hyperflex Hx Data Platform	All	All	All	All
References						
Reference	Source	Link	Tags			
Cisco HyperFlex HX Command Injection Vulnerabilities	CISCO	tools.cisco.com				
Cisco HyperFlex HX Data Platform Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com				
CVE Program record	CVE.ORG	www.cve.org	canonical			
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis			
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev			
No vendor comments have been submitted for this CVE.						
Legacy QID Mappings						
730070 Cisco HyperFlex HX Command Injection Vulnerabilities(cisco-sa-hyperflex-rce-TjjNrkpR)						

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report