



# CVE-2019-1857

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-1857
<b>State</b>	PUBLIC
<b>Assigner</b>	psirt@cisco.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-05-03 17:29:00 UTC
<b>Updated</b>	2019-05-06 13:29:00 UTC
<b>Description</b>	A vulnerability in the web-based management interface of Cisco HyperFlex HX-Series could allow an unauthenticated, remote

## Risk And Classification

**Problem Types:** CWE-352

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Hx220c Af M5	-	All	All	All
Hardware	Cisco	Hx220c Af M5	-	All	All	All
Operating System	Cisco	Hx220c Af M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx220c Af M5 Firmware	3.0(1a\)	All	All	All
Operating System	Cisco	Hx220c Af M5 Firmware	3.0(1a\)	All	All	All
Hardware	Cisco	Hx220c All Nvme M5	-	All	All	All
Hardware	Cisco	Hx220c All Nvme M5	-	All	All	All
Operating System	Cisco	Hx220c All Nvme M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx220c All Nvme M5 Firmware	3.0(1a\)	All	All	All
Operating System	Cisco	Hx220c All Nvme M5 Firmware	3.0(1a\)	All	All	All
Hardware	Cisco	Hx220c Edge M5	-	All	All	All
Hardware	Cisco	Hx220c Edge M5	-	All	All	All
Operating System	Cisco	Hx220c Edge M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx220c Edge M5 Firmware	3.0(1a\)	All	All	All
Operating System	Cisco	Hx220c Edge M5 Firmware	3.0(1a\)	All	All	All
Hardware	Cisco	Hx220c M5	-	All	All	All
Hardware	Cisco	Hx220c M5	-	All	All	All

Operating System	Cisco	Hx220c M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx220c M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx220c M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Hx240c Af M5	-	All	All	All
Hardware	Cisco	Hx240c Af M5	-	All	All	All
Operating System	Cisco	Hx240c Af M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx240c Af M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx240c Af M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Hx240c Large Form Factor	-	All	All	All
Hardware	Cisco	Hx240c Large Form Factor	-	All	All	All
Operating System	Cisco	Hx240c Large Form Factor Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx240c Large Form Factor Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx240c Large Form Factor Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Hx240c M5	-	All	All	All
Hardware	Cisco	Hx240c M5	-	All	All	All
Operating System	Cisco	Hx240c M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx240c M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Hx240c M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Ucs B200 M5	-	All	All	All
Hardware	Cisco	Ucs B200 M5	-	All	All	All
Operating System	Cisco	Ucs B200 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs B200 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs B200 M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Ucs B480 M5	-	All	All	All
Hardware	Cisco	Ucs B480 M5	-	All	All	All
Operating System	Cisco	Ucs B480 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs B480 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs B480 M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Ucs C125 M5	-	All	All	All
Hardware	Cisco	Ucs C125 M5	-	All	All	All
Operating System	Cisco	Ucs C125 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C125 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C125 M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Ucs C220 M5	-	All	All	All
Hardware	Cisco	Ucs C220 M5	-	All	All	All

Operating System	Cisco	Ucs C220 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C220 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C220 M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Ucs C240 M5	-	All	All	All
Hardware	Cisco	Ucs C240 M5	-	All	All	All
Operating System	Cisco	Ucs C240 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C240 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C240 M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Ucs C480 M5	-	All	All	All
Hardware	Cisco	Ucs C480 M5	-	All	All	All
Operating System	Cisco	Ucs C480 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C480 M5 Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C480 M5 Firmware	3.0(1a)	All	All	All
Hardware	Cisco	Ucs C480 MI	-	All	All	All
Hardware	Cisco	Ucs C480 MI	-	All	All	All
Operating System	Cisco	Ucs C480 MI Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C480 MI Firmware	3.0(1a)	All	All	All
Operating System	Cisco	Ucs C480 MI Firmware	3.0(1a)	All	All	All

## References

Reference	Source	Link
Cisco HyperFlex HX-Series Web-Based Management Interface Cross-Site Request Forgery Vulnerability	CISCO	<a href="https://tools.cisco.com">tools.cisco.com</a>
Cisco HyperFlex HX-Series CVE-2019-1857 Cross Site Request Forgery Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© 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). This site includes MITRE data granted under the following [license](https://www.mitre.org).

