CVE-2017-12226

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-12226
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-29 01:34:00 UTC
Updated	2019-10-09 23:22:00 UTC
Description	A vulnerability in the web-based Wireless Controller GUI of Cisco IOS XE Software for Cisco 5760 Wireless LAN Controller

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xe	3.7.0e	All	All	All
Operating System	Cisco	Ios Xe	3.7.1e	All	All	All
Operating System	Cisco	Ios Xe	3.7.2e	All	All	All
Operating System	Cisco	Ios Xe	3.7.3e	All	All	All
Operating System	Cisco	Ios Xe	3.7.4e	All	All	All
Operating System	Cisco	Ios Xe	3.7.5e	All	All	All
Operating System	Cisco	Ios Xe	3.7.0e	All	All	All
Operating System	Cisco	Ios Xe	3.7.1e	All	All	All
Operating System	Cisco	Ios Xe	3.7.2e	All	All	All
Operating System	Cisco	Ios Xe	3.7.3e	All	All	All
Operating System	Cisco	Ios Xe	3.7.4e	All	All	All
Operating System	Cisco	Ios Xe	3.7.5e	All	All	All

References

Reference
Cisco Catalyst 4500E Supervisor Engine 8-E Wireless Switch HTTP Request Processing Bug Lets Remote Authenticated Users Gain Elevate
Cisco IOS XE Software for Cisco 5760 WLC, Cisco Catalyst 4500E Supervisor Engine 8-E, and Cisco NGWC 3850 GUI Privilege Escalation V

Cisco IOS XE for 5760 Series Wireless LAN Controller HTTP Request Processing Bug Lets Remote Authenticated Users Gain Elevated Privil
Malformed Request
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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