



CVE-2018-0123

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

Summary

CVE	CVE-2018-0123
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-08 07:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A Path Traversal vulnerability in the diagnostic shell for Cisco IOS and IOS XE Software could allow an authenticated, local

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	16.7(1)	All	All	All
Operating System	Cisco	ios	16.7(1)	All	All	All
Operating System	Cisco	ios	16.7(1)	All	All	All
Operating System	Cisco	ios Xe	-	All	All	All
Operating System	Cisco	ios Xe	-	All	All	All

References

Reference
Cisco IOS XE Software Diagnostic Shell Path Traversal Vulnerability
Cisco IOS/IOS XE Input Validation Bug in Diagnostic Shell Lets Local Users Overwrite System Files on the Target System - SecurityTracker
Cisco IOS and IOS XE Software CVE-2018-0123 Local Arbitrary File Overwrite Vulnerability
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.

© [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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)