



CVE-2018-0100

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

Summary

CVE	CVE-2018-0100
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-18 06:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the Profile Editor of the Cisco AnyConnect Secure Mobility Client could allow an unauthenticated, local attacker to cause a denial of service (DoS) condition by sending a crafted XML request to the Profile Editor. The vulnerability is due to a buffer overflow in the Profile Editor. An attacker could exploit this vulnerability by sending a crafted XML request to the Profile Editor. A successful exploit could allow the attacker to cause a denial of service (DoS) condition by sending a crafted XML request to the Profile Editor. Cisco has released a software update to address this vulnerability. Users are advised to upgrade to the latest version of the software.

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All

References

Reference
Cisco AnyConnect Secure Mobility Client Profile Editor XML External Entity Processing Flaw Lets Remote Users Read and Write Information c
Cisco AnyConnect Profile Editor XML External Entity Injection Vulnerability
Cisco AnyConnect Profile Editor CVE-2018-0100 Local XML External Entity Injection 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.

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