



CVE-2018-15463

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

Summary

CVE	CVE-2018-15463
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-15 20:29:00 UTC
Updated	2019-10-09 23:35:00 UTC
Description	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated user to execute arbitrary code on the affected device.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine Software	2.4(0.357)	All	All	All
Application	Cisco	Identity Services Engine Software	2.4(0.357)	All	All	All
Application	Cisco	Identity Services Engine Software	2.4(0.357)	All	All	All

References

Reference	Source	Link	Tags
Cisco Identity Services Engine Multiple Cross-Site Scripting Vulnerabilities	CISCO	tools.cisco.com	Vendor Advis
Cisco Identity Services Engine Cross Site Scripting and HTML-injection Vulnerabilities	BID	www.securityfocus.com	Third Party Ac
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, an

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](#).

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