CVE-2018-0131

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

Summary

CVE	CVE-2018-0131
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-14 16:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the implementation of RSA-encrypted nonces in Cisco IOS Software and Cisco IOS XE Software could all

Risk And Classification

Problem Types: CWE-326

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios	15.5(3)s	All	All	All
Operating System	Cisco	Ios	15.5\(3\)s	All	All	All
Operating System	Cisco	Ios	15.5\(3\)s	All	All	All
Operating System	Cisco	Ios Xe	15.5(3)s	All	All	All
Operating System	Cisco	Ios Xe	15.5\(3\)s	All	All	All
Operating System	Cisco	Ios Xe	15.5\(3\)s	All	All	All

References

Reference	S
Cisco IOS/IOS XE IKEv1 Flaw Lets Remote Users Obtain Remote RSA-Encrypted IKEv1 Nonces on the Target System - SecurityTracker	S
Cisco IOS and IOS XE Software CVE-2018-0131 Information Disclosure Vulnerability	B
Cisco IOS and IOS XE Software Internet Key Exchange Version 1 RSA-Encrypted Nonces Vulnerability	C
CVE Program record	C
NVD vulnerability detail	N

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**