



CVE-2018-0131

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

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	
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.

© [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](#)