



CVE-2011-0935

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

Summary

CVE	CVE-2011-0935
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-04-14 16:55:00 UTC
Updated	2011-04-21 02:33:00 UTC
Description	The PKI functionality in Cisco IOS 15.0 and 15.1 does not prevent permanent caching of certain public keys, which allows r

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	15.0	All	All	All
Operating System	Cisco	ios	15.1	All	All	All
Operating System	Cisco	ios	15.0	All	All	All
Operating System	Cisco	ios	15.1	All	All	All

References

Reference	Source
Cisco IOS PKI Functionality Security Bypass Vulnerability	BID
Cross-Platform Release Notes for Cisco IOS Release 15.1M&T - Release 15.1(2)T Caveats [Cisco IOS 15.1M&T] - Cisco Systems	CONFII
Cisco IOS 15.1S Release Notes - Release 15.1(1)S Caveats [Cisco IOS 15.1S] - Cisco Systems	CONFII
CVE Program record	CVE.OI
NVD vulnerability detail	NVD

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](#)