



CVE-2015-0711

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

Summary

CVE	CVE-2015-0711
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-04-29 01:59:00 UTC
Updated	2015-09-10 16:07:00 UTC
Description	The hamgr service in the IPv6 Proxy Mobile (PM) implementation in Cisco StarOS 18.1.0.59776 on ASR 5000 devices allow

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Asr 5000	All	All	All	All
Hardware	Cisco	Asr 5000	All	All	All	All
Hardware	Cisco	Asr 5500	All	All	All	All
Hardware	Cisco	Asr 5500	All	All	All	All
Hardware	Cisco	Asr 5700	All	All	All	All
Hardware	Cisco	Asr 5700	All	All	All	All
Operating System	Cisco	Staros	18.1.0.59776	All	All	All
Operating System	Cisco	Staros	18.1.0.59776	All	All	All

References

Reference	Source
Cisco StarOS for Cisco ASR 5000 Series HAMGR Service Proxy Mobile IPv6 Processing Denial of Service Vulnerability	CISCO
Cisco StarOS for Cisco ASR 5000 Series Router Proxy Mobile IPv6 Bug Lets Remote Users Deny Service - SecurityTracker	SECTrack
CVE Program record	CVE.ORG
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](#)