



CVE-2016-6455

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

Summary

CVE	CVE-2016-6455
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-03 21:59:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	A vulnerability in the Slowpath of StarOS for Cisco ASR 5500 Series routers with Data Processing Card 2 (DPC2) could allow an attacker to execute arbitrary code with root privileges.

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

EPSS: 0.012430000 probability, percentile 0.793830000 (date 2026-05-08)

Problem Types: CWE-399 | unspecified

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Asr 5000 Software	18.0.0	All	All	All
Operating System	Cisco	Asr 5000 Software	18.0.0.57828	All	All	All
Operating System	Cisco	Asr 5000 Software	18.0.0.59167	All	All	All
Operating System	Cisco	Asr 5000 Software	18.0.0.59211	All	All	All
Operating System	Cisco	Asr 5000 Software	18.0.0.59219	All	All	All
Operating System	Cisco	Asr 5000 Software	18.1.0	All	All	All
Operating System	Cisco	Asr 5000 Software	18.1.0.59776	All	All	All
Operating System	Cisco	Asr 5000 Software	18.1.0.59780	All	All	All
Operating System	Cisco	Asr 5000 Software	18.1_base	All	All	All
Operating System	Cisco	Asr 5000 Software	18.3.0	All	All	All
Operating System	Cisco	Asr 5000 Software	18.3_base	All	All	All
Operating System	Cisco	Asr 5000 Software	18.4.0	All	All	All
Operating System	Cisco	Asr 5000 Software	19.0.1	All	All	All
Operating System	Cisco	Asr 5000 Software	19.0.m0.60737	All	All	All
Operating System	Cisco	Asr 5000 Software	19.0.m0.60828	All	All	All
Operating System	Cisco	Asr 5000 Software	19.0.m0.61045	All	All	All

Operating System	Cisco	Asr 5000 Software	19.1.0	All	All	All
Operating System	Cisco	Asr 5000 Software	19.1.0.61559	All	All	All
Operating System	Cisco	Asr 5000 Software	19.2.0	All	All	All
Operating System	Cisco	Asr 5000 Software	19.3.0	All	All	All
Operating System	Cisco	Asr 5000 Software	20.0.0	All	All	All
Hardware	Cisco	Asr 5500	-	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version		Platforms	
CNA	Na	Cisco StarOS 18.x Through 21.x	affected Cisco StarOS 18.x through 21.x		Not specified	

References						
Reference						
Cisco StarOS for ASR 5500 Series Routers CVE-2016-6455 Remote Denial of Service Vulnerability						
Cisco ASR 5500 Series Router Fragmented Packet Processing Bug in StarOS Slowpath Lets Remote Users Deny Service - SecurityTracker						
Cisco ASR 5500 Series with DPC2 Cards SESSMGR Denial of Service Vulnerability						
CVE Program record						
NVD vulnerability detail						

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](#)