



CVE-2011-2547

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

Summary

CVE	CVE-2011-2547
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-07-28 22:55:00 UTC
Updated	2017-08-29 01:29:00 UTC
Description	The web-based management interface on Cisco SA 500 series security appliances with software before 2.1.19 allows remo

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Sa500 Software	1.0.14	All	All	All
Application	Cisco	Sa500 Software	1.0.15	All	All	All
Application	Cisco	Sa500 Software	1.0.17	All	All	All
Application	Cisco	Sa500 Software	1.0.39	All	All	All
Application	Cisco	Sa500 Software	1.1.21	All	All	All
Application	Cisco	Sa500 Software	1.1.42	All	All	All
Application	Cisco	Sa500 Software	1.1.65	All	All	All
Application	Cisco	Sa500 Software	1.0.14	All	All	All
Application	Cisco	Sa500 Software	1.0.15	All	All	All
Application	Cisco	Sa500 Software	1.0.17	All	All	All
Application	Cisco	Sa500 Software	1.0.39	All	All	All
Application	Cisco	Sa500 Software	1.1.21	All	All	All
Application	Cisco	Sa500 Software	1.1.42	All	All	All
Application	Cisco	Sa500 Software	1.1.65	All	All	All
Application	Cisco	Sa500 Software	All	All	All	All
Hardware	Cisco	Sa520	All	All	All	All
Hardware	Cisco	Sa520	All	All	All	All

Hardware	Cisco	Sa520w	All	All	All	All
Hardware	Cisco	Sa520w	All	All	All	All
Hardware	Cisco	Sa540	All	All	All	All
Hardware	Cisco	Sa540	All	All	All	All

References

Reference

Cisco Security Advisory: Cisco SA 500 Series Security Appliances Web Management Interface Vulnerabilities - Cisco Systems

Cisco SA 500 Series Web Management Interface Two Vulnerabilities - Advisories - Community

IBM X-Force Exchange

Cisco SA500 Series Security Appliance Lets Remote Users Inject SQL Commands and Remote Authenticated Users Gain Root Privileges - S

Cisco SA 500 Series Appliances Web Management Interface Remote Command Injection 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)