CVE-2018-0414

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

Summary

CVE	CVE-2018-0414
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-05 14:29:00 UTC
Updated	2019-10-09 23:32:00 UTC
Description	A vulnerability in the web-based UI of Cisco Secure Access Control Server could allow an authenticated, remote attacker to

Risk And Classification

Problem Types: CWE-611

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Access Control Server Solution Engine	All	All	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	-	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p1	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p2	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p3	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p4	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p5	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p6	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p7	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p8	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p9	All	All
Application	Cisco	Secure Access Control Server Solution Engine	All	All	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	-	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p1	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p2	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p3	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p4	All	All

Application	Cisco	Secure Access Control Server Solution Engine	5.8	p5	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p6	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p7	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p8	All	All
Application	Cisco	Secure Access Control Server Solution Engine	5.8	p9	All	All

References

Reference
Cisco Secure Access Control System XML External Entity Processing Flaw Lets Remote Users Obtain Potentially Sensitive Information - Secu
Cisco Secure Access Control Server XML External Entity Injection Vulnerability
Malformed Request
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.