CVE-2018-1722

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

Summary

CVE	CVE-2018-1722
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-24 10:29:00 UTC
Updated	2019-10-09 23:38:00 UTC
Description	IBM Security Access Manager Appliance 9.0.4.0 and 9.0.5.0 could allow remote code execution when Advanced Access C

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Security Access Manager	9.0.4.0	All	All	All
Application	Ibm	Security Access Manager	9.0.5.0	All	All	All
Application	Ibm	Security Access Manager	9.0.4.0	All	All	All
Application	Ibm	Security Access Manager	9.0.5.0	All	All	All

References

Reference
IBM Security Access Manager CVE-2018-1722 Remote Command Injection Vulnerability
Security Bulletin: IBM Security Access Manager Appliance is affected by a remote command injection vulnerability (CVE-2018-1722)
IBM Security Access Manager Appliance Lets Remote Users Inject and Execute Arbitrary Commands on the Target System - SecurityTracker
IBM X-Force Exchange
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report