CVE-2015-6418

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-6418
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-13 03:59:00 UTC
Updated	2016-12-07 18:20:00 UTC
Description	The random-number generator on Cisco Small Business RV routers 4.x and SA500 security appliances 2.2.07 does not hav

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Rv016 Multi-wan Vpn Firmware	4.0.0.7	All	All	All
Application	Cisco	Rv016 Multi-wan Vpn Firmware	4.0.2.8	All	All	All
Application	Cisco	Rv016 Multi-wan Vpn Firmware	4.0.5.0	All	All	All
Application	Cisco	Rv016 Multi-wan Vpn Firmware	4.0.0.7	All	All	All
Application	Cisco	Rv016 Multi-wan Vpn Firmware	4.0.2.8	All	All	All
Application	Cisco	Rv016 Multi-wan Vpn Firmware	4.0.5.0	All	All	All
Application	Cisco	Rv042g Dual Gigabit Wan Vpn Firmware	4.0.0.7	All	All	All
Application	Cisco	Rv042g Dual Gigabit Wan Vpn Firmware	4.2.2.7	All	All	All
Application	Cisco	Rv042g Dual Gigabit Wan Vpn Firmware	4.2.2.8	All	All	All
Application	Cisco	Rv042g Dual Gigabit Wan Vpn Firmware	4.0.0.7	All	All	All
Application	Cisco	Rv042g Dual Gigabit Wan Vpn Firmware	4.2.2.7	All	All	All
Application	Cisco	Rv042g Dual Gigabit Wan Vpn Firmware	4.2.2.8	All	All	All
Application	Cisco	Rv042 Dual Wan Vpn Router Firmware	4.0.2.8	All	All	All
Application	Cisco	Rv042 Dual Wan Vpn Router Firmware	4.0.2.8	All	All	All
Application	Cisco	Rv082 Dual Wan Vpn Router Firmware	4.0.0.7	All	All	All
Application	Cisco	Rv082 Dual Wan Vpn Router Firmware	4.0.2.8	All	All	All
Application	Cisco	Rv082 Dual Wan Vpn Router Firmware	4.0.0.7	All	All	All

Application	Cisco	Rv082 Dual Wan Vpn Router Firmware	4.0.2.8	All	All	All
Operating System	Cisco	Sa520	2.2.07	All	All	All
Operating System	Cisco	Sa520	2.2.07	All	All	All
Operating System	Cisco	Sa520w	2.2.07	All	All	All
Operating System	Cisco	Sa520w	2.2.07	All	All	All
Operating System	Cisco	Sa540	2.2.07	All	All	All
Operating System	Cisco	Sa540	2.2.07	All	All	All

References

Reference
Cisco Small Business RV Series Weak Random Number Generation Lets Remote Users Determine TLS Session Keys on the Target System
Cisco SA500 Series Security Appliances Weak Random Number Generation Lets Remote Users Determine TLS Session Keys on the Target
Malformed Request
Cisco Small Business RV Series and SA500 Series Dual WAN VPN Router Generated Key Pair Information Disclosure 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.