



# CVE-2015-6418

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

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

## 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	<a href="#">Rv082 Dual Wan Vpn Router Firmware</a>	4.0.2.8	All	All	All
Operating System	Cisco	<a href="#">Sa520</a>	2.2.07	All	All	All
Operating System	Cisco	<a href="#">Sa520</a>	2.2.07	All	All	All
Operating System	Cisco	<a href="#">Sa520w</a>	2.2.07	All	All	All
Operating System	Cisco	<a href="#">Sa520w</a>	2.2.07	All	All	All
Operating System	Cisco	<a href="#">Sa540</a>	2.2.07	All	All	All
Operating System	Cisco	<a href="#">Sa540</a>	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

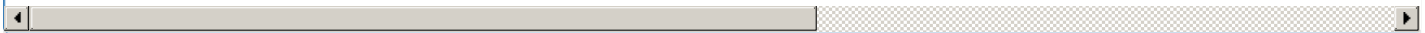
Cisco SA500 Series Security Appliances Weak Random Number Generation Lets Remote Users Determine TLS Session Keys on the Target

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.

© [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](#)