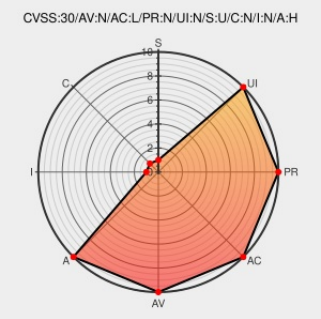
CVE-2014-9755

Published on: 01/20/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:59 PM UTC

CVE-2014-9755

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Multichannel Vpn Router 300 from Viprinet contain the following vulnerability:

The hardware VPN client in Viprinet MultichannelVPN Router 300 version 2013070830/2013080900 does not validate the remote VPN endpoint identity (through the checking of the endpoint's SSL key) before initiating the exchange, which allows remote attackers to perform a replay attack.

CVE-2014-9755 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Viprinet Multichannel VPN Router 300 Identity Verification Fail ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com	MISC packetstormsecurity.com/files/135614/Viprinet-Multichannel-VPN-Router-300-Identity-Verification-Fail.html

	text/html	
SecurityFocus	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20160203 Security Advisories
Full Disclosure: Security Advisories	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20160203 Security Advisories

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Viprinet	Multichannel Vpn Router 300	-	All	All	All
Hardware	Viprinet	Multichannel Vpn Router 300	-	All	All	All
Operating System	Viprinet	Multichannel Vpn Router 300 Firmware	2013070830	All	All	All
Operating System	Viprinet	Multichannel Vpn Router 300 Firmware	2013080900	All	All	All
Operating System	Viprinet	Multichannel Vpn Router 300 Firmware	2013070830	All	All	All
Operating System	Viprinet	Multichannel Vpn Router 300 Firmware	2013080900	All	All	All

cpe:2.3:h:viprinet:multichannel_vpn_router_300:-:*:*:*:*:*:*:*:

cpe:2.3:h:viprinet:multichannel_vpn_router_300:-:*:*:*:*:*:*:*:

cpe:2.3:o:viprinet:multichannel_vpn_router_300_firmware:2013070830:*:*:*:*:*:*:*:

cpe:2.3:o:viprinet:multichannel_vpn_router_300_firmware:2013080900:*:*:*:*:*:*:*:

cpe:2.3:o:viprinet:multichannel_vpn_router_300_firmware:2013070830:*:*:*:*:*:*:*:

cpe:2.3:o:viprinet:multichannel_vpn_router_300_firmware:2013080900:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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