



CVE-2018-3950

Published on: 11/30/2018 12:00:00 AM UTC

Last Modified on: 02/03/2023 06:02:00 PM UTC

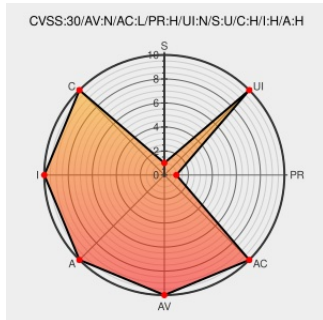
CVE-2018-3950

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [TL-r600vpn](#) from [Tp-link](#) contain the following vulnerability:

An exploitable remote code execution vulnerability exists in the ping and tracer functionality of the TP-Link TL-R600VPN HWv3 FRNv1.3.0 and HWv2 FRNv1.2.3 http server. A specially crafted IP address can cause a stack overflow, resulting in remote code execution. An attacker can send a single authenticated HTTP request to trigger this

vulnerability.

CVE-2018-3950 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Tal](#)os - [TP-Link](#) version [TP-Link TL-R600VPN HWv3 FRNv1.3.0](#) [TP-Link TL-R600VPN HWv2 FRNv1.2.3](#)

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Type	Link
-------------	------	------

Description

Tags

Link

TALOS-2018-0619 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

Third Party Advisory

talosintelligence.com

text/html

MISC

talosintelligence.com/vulnerability_reports/TALOS-2018-0619

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	Tp-link	Tl-r600vpn	2	All	All	All
Hardware	Tp-link	Tl-r600vpn	3	All	All	All
Hardware	Tp-link	Tl-r600vpn	2	All	All	All
Hardware	Tp-link	Tl-r600vpn	3	All	All	All
Operating System	Tp-link	Tl-r600vpn Firmware	1.2.3	All	All	All
Operating System	Tp-link	Tl-r600vpn Firmware	1.3.0	All	All	All
Operating System	Tp-link	Tl-r600vpn Firmware	1.2.3	All	All	All
Operating System	Tp-link	Tl-r600vpn Firmware	1.3.0	All	All	All

cpe:2.3:h:tp-link:tl-r600vpn:2:*:*:*:*:*:

cpe:2.3:h:tp-link:tl-r600vpn:3:*:*:*:*:*:

cpe:2.3:h:tp-link:tl-r600vpn:2:*:*:*:*:*:

cpe:2.3:h:tp-link:tl-r600vpn:3:*:*:*:*:*:

cpe:2.3:o:tp-link:tl-r600vpn_firmware:1.2.3:*:*:*:*:*:

cpe:2.3:o:tp-link:tl-r600vpn_firmware:1.3.0:*:*:*:*:*:

cpe:2.3:o:tp-link:tl-r600vpn_firmware:1.2.3:*:*:*:*:*:

cpe:2.3:o:tp-link:tl-r600vpn_firmware:1.3.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

© [CVE.report](#) 2023   |

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](#)