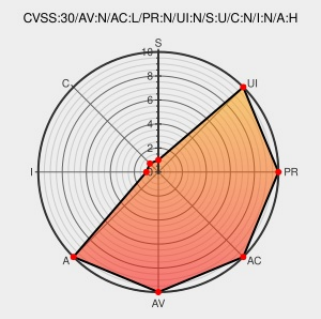
CVE-2018-15391

Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:27 PM UTC

CVE-2018-15391 - advisory for cisco-sa-20181003-phy-ipv4-dos

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



Certain versions of Remote from Cisco contain the following vulnerability:

A vulnerability in certain IPv4 fragment-processing functions of Cisco Remote PHY Software could allow an unauthenticated, remote attacker to impact traffic passing through a device, potentially causing a denial of service (DoS) condition. The vulnerability is due to the affected software not validating and calculating certain numerical values in IPv4 packets that are sent to an affected device. An attacker could exploit this vulnerability by sending malformed IPv4 traffic to an affected device. A successful exploit could allow the attacker to disrupt the flow of certain IPv4 traffic passing through an affected device, which could result in a DoS condition.

CVE-2018-15391 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Cisco** - **Cisco Remote PHY** version **n/a**

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: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Cisco Remote PHY IPv4 Fragment Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20181003 Cisco Remote PHY IPv4 Fragment Denial of Service Vulnerability

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Remote	phy	-	All	All
Application	Cisco	Remote	phy	-	All	All

cpe:2.3:a:cisco:remote:phy:-:*:*:*:*:*:*:*

cpe:2.3:a:cisco:remote:phy:-:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→