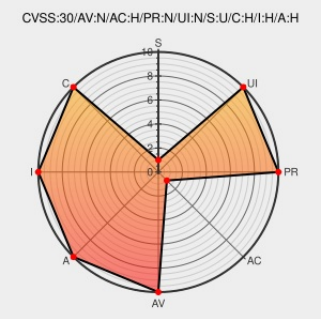
CVE-2019-15958

Published on: 11/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15958 - advisory for cisco-sa-20191106-pi-epn-codex

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



Certain versions of Evolved Programmable Network Manager from Cisco contain the following vulnerability:

A vulnerability in the REST API of Cisco Prime Infrastructure (PI) and Cisco Evolved Programmable Network Manager (EPNM) could allow an unauthenticated remote attacker to execute arbitrary code with root privileges on the underlying operating system. The vulnerability is due to insufficient input validation during the initial High Availability (HA) configuration and registration process of an affected device. An attacker could exploit this vulnerability by uploading a malicious file during the HA registration period. A successful exploit could allow the attacker to execute arbitrary code with root-level privileges on the underlying operating system. Note: This vulnerability can only be exploited during the HA registration period. See the Details section for more information.

CVE-2019-15958 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as CRITICAL severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco Prime Infrastructure** version **n/a**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20191106 Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution 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	Evolved Programmable Network Manager	All	All	All	All
Application	Cisco	Evolved Programmable Network Manager	All	All	All	All
Application	Cisco	Prime Infrastructure	All	All	All	All
Application	Cisco	Prime Infrastructure	3.6	All	All	All
Application	Cisco	Prime Infrastructure	All	All	All	All
Application	Cisco	Prime Infrastructure	3.6	All	All	All

cpe:2.3:a:cisco:evolved_programmable_network_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:evolved_programmable_network_manager:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:prime_infrastructure:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:prime_infrastructure:3.6:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:prime_infrastructure:*:*:*:*:*:*:*:*:

cpe:2.3:a:cisco:prime_infrastructure:3.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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