



CVE-2018-11750

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2018-11750 |
| State | PUBLIC |
| Assigner | security@puppet.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-10-02 19:29:00 UTC |
| Updated | 2019-01-02 15:09:00 UTC |
| Description | Previous releases of the Puppet cisco_ios module did not validate a host's identity before starting a SSH connection. As of |

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|------------------------|----------------------------------|---------|--------|---------|----------|
| Application | Puppet | Cisco Ios Module | All | All | All | All |
| Application | Puppet | Cisco Ios Module | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|--|---------------------|
| CVE-2018-11750 - Cisco IOS Module host validation issue Puppet | CONFIRM | puppet.com | Vendor Advisory |
| IBM X-Force Exchange | MISC | exchange.xforce.ibmcloud.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)