



CVE-2018-1147

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-1147
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-18 22:29:00 UTC
Updated	2018-06-19 15:32:00 UTC
Description	In Nessus before 7.1.0, a XSS vulnerability exists due to improper input validation. A remote authenticated attacker could c

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tenable	Nessus	All	All	All	All
Application	Tenable	Nessus	All	All	All	All

References

Reference
Tenable Nessus Bugs Let Remote Authenticated Users Bypass Session Security and Conduct Cross-Site Scripting Attacks - SecurityTracker
[R1] Nessus 7.1.0 Fixes Multiple Vulnerabilities - Security Advisory Tenable™
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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