



CVE-2017-7535

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

Summary

CVE	CVE-2017-7535
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-26 13:29:00 UTC
Updated	2019-10-09 23:29:00 UTC
Description	foreman before version 1.16.0 is vulnerable to a stored XSS in organizations/locations assignment to hosts. Exploiting this i

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Theforeman	Foreman	All	All	All	All
Application	Theforeman	Foreman	All	All	All	All

References

Reference	Source	Link	Tags
oss-sec: Foreman 1.1+ stored XSS in organizations/locations assignment to hosts	MLIST	seclists.org	Mailir
Foreman CVE-2017-7535 Cross Site Scripting Vulnerability	BID	www.securityfocus.com	Third
1463300 – (CVE-2017-7535) CVE-2017-7535 foreman: XSS in the manage organization page	CONFIRM	bugzilla.redhat.com	Issue
Bug #20963: CVE-2017-7535: stored XSS in the manage organization page - Foreman	CONFIRM	projects.theforeman.org	Vend
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)