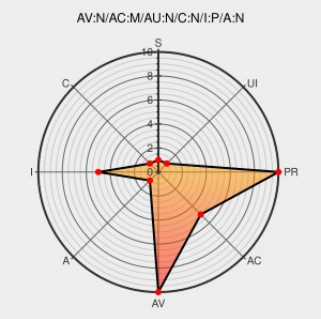
CVE-2015-7518

Published on: 12/17/2015 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:15:00 PM UTC

CVE-2015-7518

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



Certain versions of Foreman from Theforeman contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in information popups in Foreman before 1.10.0 allow remote attackers to inject arbitrary web script or HTML via (1) global parameters, (2) smart class parameters, or (3) smart variables in the (a) host or (b) hostgroup edit forms.

CVE-2015-7518 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - CVE-2015-7518: Foreman stored XSS in parameter information popup	www.openwall.com text/html	MLIST [oss-security] 20151209 CVE-2015-7518: Foreman stored XSS in parameter information popup
CVE-2015-7518 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2015-7518
1285728 – (CVE-2015-7518) CVE-2015-7518 foreman: Stored XSS vulnerability in smart class parameters/variables	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1285728
Bug #12611: CVE-2015-7518 - Smart class parameters/variables shown on host edit allows stored XSS in description - Foreman	projects.theforeman.org text/html	CONFIRM projects.theforeman.org/issues/12611
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2016:0174

Foreman :: Security	Vendor Advisory theforeman.org text/html	CONFIRM theforeman.org/security.html#2015-7518

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:theforeman:foreman:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→