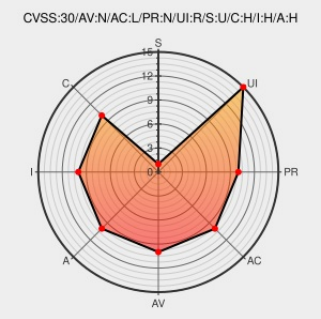
CVE-2016-3728

Published on: 05/20/2016 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:20:00 PM UTC

CVE-2016-3728

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



Certain versions of Foreman from Theforeman contain the following vulnerability:

Eval injection vulnerability in tftp_api.rb in the TFTP module in the Smart-Proxy in Foreman before 1.10.4 and 1.11.x before 1.11.2 allows remote attackers to execute arbitrary code via the PXE template type portion of the PATH_INFO to tftp/.

CVE-2016-3728 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Bug #14931: CVE-2016-3728 - Arbitrary code execution via TFTP file variant parameter - Smart Proxy - Foreman	projects.theforeman.org text/html	CONFIRM projects.theforeman.org/issues/14931
CVE-2016-3728 - Red Hat Customer Portal	access.redhat.com	MISC access.redhat.com/security/cve/CVE-2016-3728

	text/html	
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHBA-2016:1501
Foreman :: Security	Vendor Advisory theforeman.org text/html	CONFIRM theforeman.org/security.html#2016-3728
Fixes #14931 - TFTP class instantiating fixed · theforeman/smart-proxy@eef532a · GitHub	github.com text/html	CONFIRM github.com/theforeman/smart-proxy/commit/eef532aa668d656b9d61d9c6edf7c2505f3f43c7
oss-security - CVE-2016-3728: remote code execution in Foreman smart proxy TFTP API	www.openwall.com text/html	MLIST [oss-security] 20160519 CVE-2016-3728: remote code execution in Foreman smart proxy TFTP API
1333378 – (CVE-2016-3728) CVE-2016-3728 foreman: Missing input validation in Smart Proxy allows RCE via TFTP file variant parameter	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1333378

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	1.10.3	All	All	All
Application	Theforeman	Foreman	1.11.0	All	All	All
Application	Theforeman	Foreman	1.11.0	rc1	All	All
Application	Theforeman	Foreman	1.11.0	rc2	All	All
Application	Theforeman	Foreman	1.11.0	rc3	All	All
Application	Theforeman	Foreman	1.11.1	All	All	All
Application	Theforeman	Foreman	1.10.3	All	All	All
Application	Theforeman	Foreman	1.11.0	All	All	All
Application	Theforeman	Foreman	1.11.0	rc1	All	All
Application	Theforeman	Foreman	1.11.0	rc2	All	All
Application	Theforeman	Foreman	1.11.0	rc3	All	All
Application	Theforeman	Foreman	1.11.1	All	All	All

cpe:2.3:a:theforeman:foreman:1.10.3:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.1:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.10.3:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:*:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.0:rc3:*:*:*:*:*:*:

cpe:2.3:a:theforeman:foreman:1.11.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→