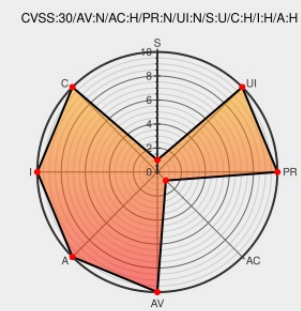
CVE-2016-3693

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

Last Modified on: 02/12/2023 11:18:00 PM UTC

CVE-2016-3693

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



Certain versions of Safemode from Safemode Project contain the following vulnerability:

The Safemode gem before 1.2.4 for Ruby, when initialized with a delegate object that is a Rails controller, allows context-dependent attackers to obtain sensitive information via the inspect method.

CVE-2016-3693 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
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
Foreman :: Security	theforeman.org text/html	CONFIRM theforeman.org/security.html#2016-3693
1327471 – (CVE-2016-3693) CVE-2016-3693 foreman:	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1327471

inspect in a provisioning template exposes sensitive controller information		
Remove `inspect` from allowed methods · svenfuchs/safemode@0f764a1 · GitHub	github.com text/html	CONFIRM github.com/svenfuchs/safemode/commit/0f764a1720a3a68fd2842e21377c8bfa
oss-security - CVE-2016-3693: Foreman application information leakage through templates	www.openwall.com text/html	MLIST [oss-security] 20160420 CVE-2016-3693: Foreman application inform leakage through templates
Fixes #14635 - bump safemode version to fix the unwanted inspect issue · theforeman/foreman@82f9b93 · GitHub	github.com text/html	CONFIRM github.com/theforeman/foreman/commit/82f9b93c54f72c5814df6bab7fad057ea
CVE-2016-3693 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2016-3693
CVE-2016-3693 (safemode): Safemode Gem for Ruby is vulnerable to information disclosure - RubySec	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM rubysec.com/advisories/CVE-2016-3693/
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:0336
Bug #14635: CVE-2016-3693 - `inspect` in a provisioning template exposes sensitive controller information - Foreman	projects.theforeman.org text/html	CONFIRM projects.theforeman.org/issues/14635

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Safemode Project	Safemode	All	All	All	All

cpe:2.3:a:safemode_project:safemode:*:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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