

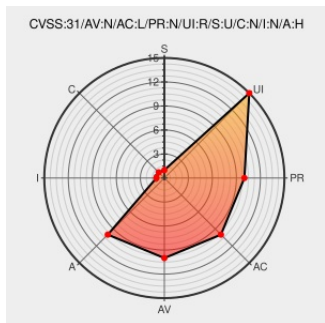


CVE-2014-3590

Published on: 01/02/2020 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:09 AM UTC

CVE-2014-3590

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Satellite](#) from [Redhat](#) contain the following vulnerability:

Versions of Foreman as shipped with Red Hat Satellite 6 does not check for a correct CSRF token in the logout action. Therefore, an attacker can log out a user by having them view specially crafted content.

CVE-2014-3590 has been assigned by [secalert@redhat.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Red Hat Satellite 6](#) - [Red Hat Satellite 6](#) version = 6

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
CVE-2014-3590 - Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	MISC access.redhat.com/security/cve/cve-2014-3590

CVE-2014-3590

Third Party Advisory

security-tracker.debian.org

text/html

MISC

security-tracker.debian.org/tracker/CVE-2014-3590

Bug 1128108 – CVE-2014-3590 rhn_satellite_6: cross-site request forgery (CSRF) can force logout

Issue Tracking

Vendor Advisory

bugzilla.redhat.com

text/html

MISC

bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-3590

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Satellite	6.0	All	All	All
Application	Redhat	Satellite	6.0	All	All	All

cpe:2.3:a:redhat:satellite:6.0:*:*:*:*:*:

cpe:2.3:a:redhat:satellite:6.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →