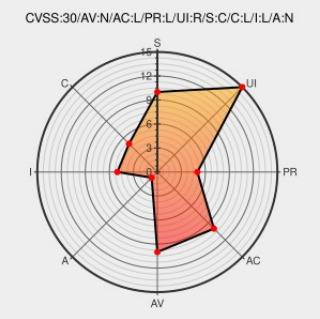
CVE-2017-7514

Published on: 07/30/2018 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:30:00 PM UTC

CVE-2017-7514

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



Certain versions of Satellite from Redhat contain the following vulnerability:

A cross-site scripting (XSS) flaw was found in how the failed action entry is processed in Red Hat Satellite before version 5.8.0. A user able to specify a failed action could exploit this flaw to perform XSS attacks against other Satellite users.

CVE-2017-7514 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Red Hat** - **Red Hat Satellite** version **= 5.8.0**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
1458052 – (CVE-2017-7514) CVE-2017-7514 SAT 5 XSS in the Failed Systems page	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1458052

CVE-2017-7514 - Red Hat Customer Portal	access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2017-7514
Red Hat Customer Portal	Vendor Advisory access.redhat.com text/html	REDHAT RHSA-2017:1558
1458052 – (CVE-2017-7514) CVE-2017-7514 SAT 5 XSS in the Failed Systems page	Issue Tracking Vendor Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-7514

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	All	All	All	All
Application	Redhat	Satellite	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→