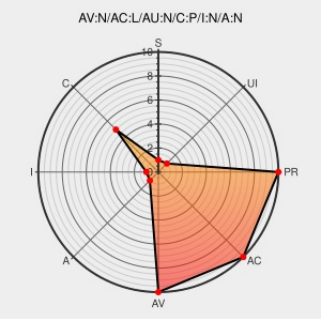
CVE-2013-2056

Published on: 07/31/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:14 AM UTC

CVE-2013-2056

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



Certain versions of Network Satellite from Redhat contain the following vulnerability:

The Inter-Satellite Sync (ISS) operation in Red Hat Network (RHN) Satellite 5.3, 5.4, and 5.5 does not properly check client "authenticity," which allows remote attackers to obtain channel content by skipping the initial authentication call.

CVE-2013-2056 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
404 Not Found	www.osvdb.org, text/html, Inactive Link, Not Archived	OSVDB 93566
About Secunia Research | Flexera	Vendor Advisory, secunia.com, Depreciated Link, text/html	SECUNIA 53487
Red Hat Customer Portal	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:0848

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	Network Satellite	5.3	All	All	All
Application	Redhat	Network Satellite	5.4	All	All	All
Application	Redhat	Network Satellite	5.5	All	All	All
Application	Redhat	Network Satellite	5.3	All	All	All
Application	Redhat	Network Satellite	5.4	All	All	All
Application	Redhat	Network Satellite	5.5	All	All	All
Application	Redhat	Satellite	5.3	All	All	All
Application	Redhat	Satellite	5.4	All	All	All
Application	Redhat	Satellite	5.5	All	All	All

cpe:2.3:a:redhat:network_satellite:5.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:network_satellite:5.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:network_satellite:5.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:network_satellite:5.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:network_satellite:5.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:network_satellite:5.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:satellite:5.3:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:satellite:5.4:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:satellite:5.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

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