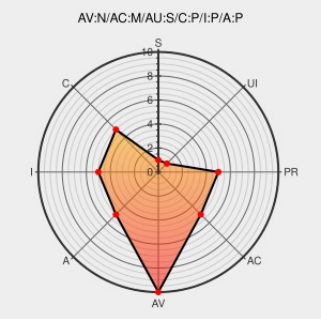
CVE-2013-4548

Published on: 11/08/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:28 PM UTC

CVE-2013-4548

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



Certain versions of Openssh from Openbsd contain the following vulnerability:

The mm_newkeys_from_blob function in monitor_wrap.c in sshd in OpenSSH 6.2 and 6.3, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address.

CVE-2013-4548 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
oss-security - Re: CVE Request - OpenSSH	openwall.com text/html	MLIST [oss-security] 20131107 Re: CVE Request - OpenSSH
USN-2014-1: OpenSSH vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2014-1
[security-announce] openSUSE-SU-2013:1726-1: important: openssh: securit	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1726
	Vendor Advisory www.openssh.com text/x-diff	CONFIRM www.openssh.com/txt/gcmrekey.adv
'[security bulletin] HPSBUX03188 SSRT101487 rev.1 - HP-UX running HP	marc.info	HP SSRT101487

Secure Shell, Remote Denial of S' - MARC text/html

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	Openbsd	Openssh	6.2	All	All	All
Application	Openbsd	Openssh	6.3	All	All	All
Application	Openbsd	Openssh	6.2	All	All	All
Application	Openbsd	Openssh	6.3	All	All	All

cpe:2.3:a:openbsd:openssh:6.2:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:6.3:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:6.2:*:*:*:*:*:*:*:

cpe:2.3:a:openbsd:openssh:6.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→