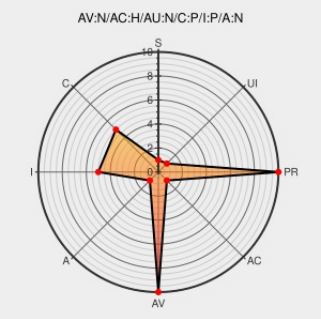
CVE-2013-4566

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

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

CVE-2013-4566

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



Certain versions of Mod Nss from Mod Nss Project contain the following vulnerability:

mod_nss 1.0.8 and earlier, when NSSVerifyClient is set to none for the server/vhost context, does not enforce the NSSVerifyClient setting in the directory context, which allows remote attackers to bypass intended access restrictions.

CVE-2013-4566 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
openSUSE-SU-2013:1956-1: moderate: update for apache2-mod_nss	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1956
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:1779
1016832 – (CVE-2013-4566) CVE-2013-4566 mod_nss: incorrect handling of NSSVerifyClient in directory context	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1016832

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mod Nss Project	Mod Nss	1.0	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.2	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.3	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.4	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.5	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.6	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.7	All	All	All
Application	Mod Nss Project	Mod Nss	1.0	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.2	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.3	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.4	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.5	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.6	All	All	All
Application	Mod Nss Project	Mod Nss	1.0.7	All	All	All
Application	Mod Nss Project	Mod Nss	All	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	5	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

cpe:2.3:a:mod_nss_project:mod_nss:1.0:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0.2:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0.3:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0.4:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0.5:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0.6:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0.7:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0:*:*:*:*:*:*:*

cpe:2.3:a:mod_nss_project:mod_nss:1.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mod_nss_project:mod_nss:1.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:mod_nss_project:mod_nss:1.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:mod_nss_project:mod_nss:1.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:mod_nss_project:mod_nss:1.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:mod_nss_project:mod_nss:1.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:mod_nss_project:mod_nss:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:5:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→