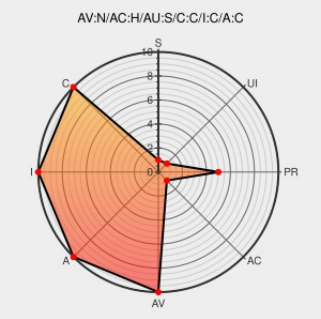
CVE-2011-3640

Published on: 10/27/2011 12:00:00 AM UTC

Last Modified on: 02/12/2023 08:15:00 PM UTC

CVE-2011-3640

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



Certain versions of Macos from Apple contain the following vulnerability:

** DISPUTED ** Untrusted search path vulnerability in Mozilla Network Security Services (NSS), as used in Google Chrome before 17 on Windows and Mac OS X, might allow local users to gain privileges via a Trojan horse pkcs11.txt file in a top-level directory. NOTE: the vendor's response was "Strange behavior, but we're not treating this as a security bug."

CVE-2011-3640 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
641052 – (CVE-2011-3640) NSS_NoDB_Init should not try to open /pkcs11.txt and /secmod.db	Issue Tracking, Patch, Third Party Advisory, bugzilla.mozilla.org, text/html	MISC bugzilla.mozilla.org/show_bug.cgi?id=641052
ACROS Security Blog: Google Chrome pkcs11.txt File Planting	Exploit, Third Party Advisory, blog.acrossecurity.com, text/html	MISC blog.acrossecurity.com/2011/10/google-chrome-pkcs11txt-file-planting.html
No Description Provided	Broken Link, hermes.opensuse.org	SUSE openSUSE-SU-2012:0030

	Inactive Link Not Archived	
Issue 97426 - chromium - Security: pkcs11.txt file planting leads to remote code execution outside sandbox - An open-source browser project to help move the web forward. - Google Project Hosting	Exploit Issue Tracking Patch Vendor Advisory code.google.com text/html	MISC code.google.com/p/chromium/issues/detail?id=97426
No Description Provided	Broken Link hermes.opensuse.org Inactive Link Not Archived	SUSE openSUSE-SU-2012:0063
Google Chrome pkcs11.txt File Planting - CXSecurity.com	Third Party Advisory securityreason.com text/html	SREASON 8483
Repository / Oval Repository	Third Party Advisory oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:13414

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
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Application	Google	Chrome	All	All	All	All
Application	Google	Chrome	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:o:apple:macos:-:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→