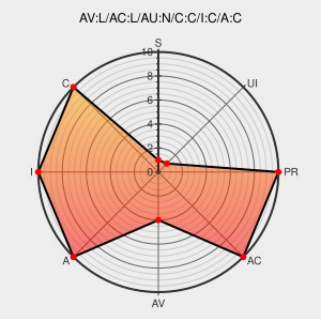
CVE-2012-3485

Published on: 08/26/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:16 PM UTC

CVE-2012-3485

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



Certain versions of Tunnelblick from Google contain the following vulnerability:

Tunnelblick 3.3beta20 and earlier relies on argv[0] to determine the name of an appropriate (1) kernel module pathname or (2) executable file pathname, which allows local users to gain privileges via an execl system call.

CVE-2012-3485 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20120811 OS X Local Root: Silly SUID Helper in Tunnel Blick
Setuid Tunnelblick Privilege Escalation	www.exploit-db.com, Proof of Concept, text/html	EXPLOIT-DB 24578
Pwnnel-Blicker - A local root exploit for the popular OS X OpenVPN manager, Tunnel Blick.	git.zx2c4.com, text/html	MISC git.zx2c4.com/Pwnnel-Blicker/tree/pwnnel-blicker-for-kids.sh
Issue 212 - tunnelblick - Security problem (race condition in SUID code) - OpenVPN GUI for Mac OS X - Google Project Hosting	code.google.com, text/html	CONFIRM code.google.com/p/tunnelblick/issues/detail?id=212
oss-security - Re: Tunnel Blick: Multiple Vulnerabilities to Local Root and DoS (OS X)	www.openwall.com, text/html	MLIST [oss-security] 20120812 Re: Tunnel Blick: Multiple Vulnerabilities to Local

Root and DoS (OS X)

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	Google	Tunnelblick	All	All	All	All

cpe:2.3:a:google:tunnelblick:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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