



CVE-2011-1080

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2011-1080
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-21 23:55:00 UTC
Updated	2023-02-13 04:29:00 UTC
Description	The do_replace function in net/bridge/netfilter/ebtables.c in the Linux kernel before 2.6.39 does not ensure that a certain na

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	2.6.38	All	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc8	All	All
Operating System	Linux	Linux Kernel	2.6.38.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.38	All	All	All

Operating System	Linux	Linux Kernel	2.6.38	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.38	rc8	All	All
Operating System	Linux	Linux Kernel	2.6.38.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.38.7	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References						
Reference				Source	Link	Tags
kernel/git/torvalds/linux.git - Linux kernel source tree				CONFIRM	git.kernel.org	
access.redhat.com				REDHAT	rhn.redhat.com	
404 Not Found				CONFIRM	ftp.osuosl.org	
bridge: netfilter: fix information leak · torvalds/linux@d846f71 · GitHub				CONFIRM	github.com	
681262 – (CVE-2011-1080) CVE-2011-1080 kernel: ebttables stack infoleak				CONFIRM	bugzilla.redhat.com	
oss-security - Re: CVE request: kernel: two bluetooth and one ebttables infoleaks/DoSes				MLIST	www.openwall.com	
kernel/git/torvalds/linux.git - Linux kernel source tree				MISC	git.kernel.org	
ASA-2011-208 (RHSA-2011-0833)				CONFIRM	downloads.avaya.com	
CVE Program record				CVE.ORG	www.cve.org	canonical
NVD vulnerability detail				NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)