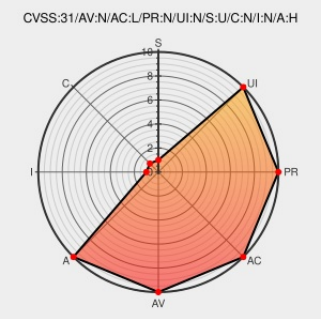
CVE-2011-2189

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

Last Modified on: 02/13/2023 04:30:00 AM UTC

CVE-2011-2189

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

net/core/net_namespace.c in the Linux kernel 2.6.32 and earlier does not properly handle a high rate of creation and cleanup of network namespaces, which makes it easier for remote attackers to cause a denial of service (memory consumption) via requests to a daemon that requires a separate namespace per connection, as demonstrated by vsftpd.

CVE-2011-2189 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
oss-security - Re: CVE Request -- vsftpd -- Do not create	Mailing List Third Party Advisory	MLIST [oss-security] 20110606 Re: CVE Request -- vsftpd -- Do not create network namespace per connection

network namespace per connection	www.openwall.com text/html	
kernel/git/torvalds/linux.git - Linux kernel source tree	web.archive.org text/html Inactive Link Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=f875bae065334907796da12523f9df85c89f5712
No Description Provided	Broken Link kerneltrap.org Inactive Link Not Archived	MLIST [git-commits-head] 20091208 net: Automatically allocate per namespace data.
oss-security - Re: CVE Request -- vsftpd -- Do not create network namespace per connection	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20110606 Re: CVE Request -- vsftpd -- Do not create network namespace per connection
Debian -- Security Information -- DSA-2305-1 vsftpd	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-2305
404 Not Found	Broken Link ie.archive.ubuntu.com text/html Inactive Link Not Archived	CONFIRM ie.archive.ubuntu.com/linux/kernel/v2.6/ChangeLog-2.6.33
Bug #720095 “vsftpd causes a vmalloc space leak in Lucid” : Bugs : “linux” package : Ubuntu	Exploit Third Party Advisory bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/ubuntu/+source/linux/+bug/720095
git.neil.brown.name Git	Broken Link neil.brown.name text/xml Inactive Link Not Archived	MISC neil.brown.name/git?p=linux-2.6%3Ba=patch%3Bh=2b035b39970740722598f7a9d548835f9bdd730f
USN-1288-1: vsftpd vulnerability | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-1288-1
kernel/git/torvalds/linux.git - Linux kernel source tree	Mailing List Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git%3Ba=commit%3Bh=2b035b39970740722598f7a9d548835f9bdd730f
[RFC/Review] Prevent network namespace memory exhaution - Patchwork	Mailing List Patch Third Party Advisory patchwork.ozlabs.org text/html	CONFIRM patchwork.ozlabs.org/patch/88217/
#629373 - Remote DoS with vsftpd on Linux 2.6.32 - Debian Bug report logs	Exploit Mailing List Third Party Advisory bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=629373
Bug 711245 – CVE-2011-2189 kernel: net_ns: oom killer fires because of slow net_ns cleanup	Exploit Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=711245

Bug 711134 – vsftpd: Do not create network namespace per connection	Exploit Issue Tracking Third Party Advisory bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=711134

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	10.10	All	All	All
Operating System	Canonical	Ubuntu Linux	11.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All

Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating System	Redhat	Enterprise Mrg	2.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All

- cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:11.04:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:10.10:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:11.04:*:*:*:*:*:*:*:
- cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:
- cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_linux:6.0:*:*:*:*:*:*:*:
- cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:
- cpe:2.3:o:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:
- cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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