



CVE-2015-3636

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

Summary

CVE	CVE-2015-3636
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-06 01:59:00 UTC
Updated	2019-04-22 17:48:00 UTC
Description	The ping_unhash function in net/ipv4/ping.c in the Linux kernel before 4.0.3 does not initialize a certain list data structure du

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Debian	Debian Linux	7.0	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

References

Reference	Source	Link
[security-announce] SUSE-SU-2015:1489-1: important: Live patch for the L	SUSE	lists.
USN-2634-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.k
[security-announce] SUSE-SU-2015:1491-1: important: Live patch for the L	SUSE	lists.
[security-announce] SUSE-SU-2015:1487-1: important: Live patch for the L	SUSE	lists.
USN-2631-1: Linux kernel vulnerabilities Ubuntu	UBUNTU	www
oss-security - CVE request for a fixed bug existed in all versions of linux kernel from KeenTeam	MLIST	www

Linux Kernel CVE-2015-3636 Local Privilege Escalation Vulnerability	BID	www
[security-announce] SUSE-SU-2015:1224-1: important: Security update for	SUSE	lists.
Red Hat Customer Portal	REDHAT	rh.n.r
[SECURITY] Fedora 21 Update: kernel-3.19.7-200.fc21	FEDORA	lists.
Red Hat Customer Portal	REDHAT	rh.n.r
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.0.3	CONFIRM	www
[SECURITY] Fedora 20 Update: kernel-3.19.8-100.fc20	FEDORA	lists.
[security-announce] SUSE-SU-2015:1478-1: important: Security update for	SUSE	lists.
Red Hat Customer Portal	REDHAT	rh.n.r
Linux ping Use-After-Free Memory Error Lets Local Users Deny Service and Gain Elevated Privileges - SecurityTracker	SECTrack	www
Red Hat Customer Portal	REDHAT	rh.n.r
USN-2633-1: Linux kernel (Trusty HWE) vulnerabilities Ubuntu	UBUNTU	www
Oracle Linux Bulletin - January 2016	CONFIRM	www
ipv4: Missing sk_nulls_node_init() in ping_unhash(). · torvalds/linux@a134f08 · GitHub	CONFIRM	githu
Red Hat Customer Portal	REDHAT	rh.n.r
Bug 1218074 – CVE-2015-3636 kernel: ping sockets: use-after-free leading to local privilege escalation	CONFIRM	bugz
[security-announce] openSUSE-SU-2015:1382-1: important: Security update	SUSE	lists.
USN-2632-1: Linux kernel (OMAP4) vulnerabilities Ubuntu	UBUNTU	www
[SECURITY] Fedora 22 Update: kernel-4.0.2-300.fc22	FEDORA	lists.
[security-announce] SUSE-SU-2015:1488-1: important: Live patch for the L	SUSE	lists.
Debian -- Security Information -- DSA-3290-1 linux	DEBIAN	www
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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