CVE-2015-3290

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-3290
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-31 10:59:00 UTC
Updated	2024-02-05 20:15:00 UTC
Description	arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform improperly relies on espfix64 during neste

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org
USN-2687-1: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.c
Debian -- Security Information -- DSA-3313-1 linux	DEBIAN	www.debian.c
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.1.6	CONFIRM	www.kernel.o
USN-2691-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.c
oss-security - Linux x86_64 NMI security issues	MLIST	www.openwa
USN-2690-1: Linux kernel (Vivid HWE) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.c
Linux espfix64 - Privilege Escalation Nested NMIs Interrupting - Exploits Database	EXPLOIT-DB	www.exploit-c
oss-security - CVE-2015-3290: Linux privilege escalation due to nested NMIs interrupting espfix64	MLIST	www.openwa
x86/nmi/64: Switch stacks on userspace NMI entry · torvalds/linux@9b6e6a8 · GitHub	CONFIRM	github.com
Linux Kernel 'x86/entry/entry_64.S' Local Privilege Escalation Vulnerability	BID	www.securityf
USN-2688-1: Linux kernel vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.c

[security-announce] openSUSE-SU-2015:1382-1: important: Security update	SUSE	lists.opensuse
USN-2689-1: Linux kernel (Utopic HWE) vulnerabilities | Ubuntu	UBUNTU	www.ubuntu.c
Bug 1243465 – CVE-2015-3290 kernel: x86: nested NMI handler and espfix64 interaction privilege escalation	CONFIRM	bugzilla.redha
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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