CVE-2018-8897

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-8897
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-05-08 18:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM)

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	17.10	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All
Application	Citrix	Xenserver	6.2.0	All	All	All
Application	Citrix	Xenserver	6.5	All	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	7.1	All	All	All
Application	Citrix	Xenserver	7.2	All	All	All
Application	Citrix	Xenserver	7.3	All	All	All
Application	Citrix	Xenserver	7.4	All	All	All
Application	Citrix	Xenserver	6.0.2	All	All	All

Application	Citrix	Xenserver	6.2.0	All	All	All
Application	Citrix	Xenserver	6.5	All	All	All
Application	Citrix	Xenserver	7.0	All	All	All
Application	Citrix	Xenserver	7.1	All	All	All
Application	Citrix	Xenserver	7.2	All	All	All
Application	Citrix	Xenserver	7.3	All	All	All
Application	Citrix	Xenserver	7.4	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Freebsd	Freebsd	All	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Virtualization Manager	3.0	All	All	All
Operating System	Redhat	Enterprise Virtualization Manager	3.0	All	All	All
Operating System	Synology	Diskstation Manager	5.2	All	All	All
Operating System	Synology	Diskstation Manager	6.0	All	All	All
Operating System	Synology	Diskstation Manager	6.1	All	All	All
Operating System	Synology	Diskstation Manager	5.2	All	All	All
Operating System	Synology	Diskstation Manager	6.0	All	All	All
Operating System	Synology	Diskstation Manager	6.1	All	All	All
Application	Synology	Skynas	-	All	All	All
Application	Synology	Skynas	-	All	All	All
Operating System	Xen	Xen	-	All	All	All
Operating System	Xen	Xen	-	All	All	All

References

Reference
x86/entry/64: Don't use IST entry for #BP stack · torvalds/linux@d8ba61b · GitHub

Red Hat Customer Portal

kernel/git/torvalds/linux.git - Linux kernel source tree

CVE-2018-8897 x86 Debug Exception Vulnerability in NetApp Products | NetApp Product Security

Red Hat Customer Portal

Red Hat Customer Portal

Apple macOS/OS X LinkPresentation, Crash Reporter, and Kernel Bugs Let Remote Users Spoof the User Interface and Local Users Gain Ele

Huawei - Building a Fully Connected, Intelligent World

FreeBSD Kernel Debug Exception Handling Flaw Lets Local Users Gain Elevated Privileges - SecurityTracker

Spurious #DB exceptions with the "MOV SS" and "POP SS" instructions (CVE-2018-8897)

Red Hat Customer Portal

[SECURITY] [DLA 1577-1] xen security update

Debian -- Security Information -- DSA-4201-1 xen

Red Hat Customer Portal

Red Hat Customer Portal

Citrix XenServer Multiple Security Updates

Debian -- Security Information -- DSA-4196-1 linux

DCIM Support

Microsoft Windows - 'POP/MOV SS' Privilege Escalation - Windows local Exploit

CERT Vulnerability Notes Database

[SECURITY] [DLA 1392-1] linux security update

XSA-260 - Xen Security Advisories

Xen Debug Exception Handling Flaw Lets Local Users on a PV Guest System Gain Elevated Privileges on the Host System - SecurityTracker

Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

www.freebsd.org/security/advisories/FreeBSD-SA-18:06.debugreg.asc

oss-security - CVE-2018-8897: #DB exceptions that are deferred by MOV SS or POP SS may cause unexpected behavior

[SECURITY] [DLA 1383-1] xen security update

portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8897

Synology Inc.

1567074 – (CVE-2018-8897) CVE-2018-8897 Kernel: error in exception handling leads to DoS

Microsoft Windows Kernel CVE-2018-8897 Local Privilege Escalation Vulnerability

selftests/x86: Add mov_to_ss - Patchwork

oss-security - Xen Security Advisory 260 (CVE-2018-8897) - x86: mishandling of debug exceptions

Microsoft Windows - POP/MOV SS Local Privilege Elevation (Metasploit) - Windows local Exploit

GitHub - can1357/CVE-2018-8897: Arbitrary code execution with kernel privileges using CVE-2018-8897.

Windows Kernel Multiple Flaws Let Local Users Bypass Security Restictions, Obtain Potentially Sensitive Information, and Gain Elevated Privi
Linux Kernel Debug Exception Handling Flaw Lets Local Users Cause Denial of Service Conditions on the Target System - SecurityTracker
USN-3641-2: Linux kernel vulnerabilities | Ubuntu security notices
Red Hat Customer Portal
[base] Revision 333368
About the security content of Security Update 2018-001 - Apple Support
Red Hat Customer Portal
Red Hat Customer Portal
Red Hat Customer Portal
USN-3641-1: Linux kernel vulnerabilities | Ubuntu security notices
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500749 Alpine Linux Security Update for xen
504526 Alpine Linux Security Update for xen