



# CVE-2018-12127

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

## Summary

<b>CVE</b>	CVE-2018-12127
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@intel.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-05-30 16:29:00 UTC
<b>Updated</b>	2023-11-07 02:52:00 UTC
<b>Description</b>	Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	29	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Microarchitectural Load Port Data Sampling</a>	-	All	All	All
Hardware	<a href="#">Intel</a>	<a href="#">Microarchitectural Load Port Data Sampling</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Microarchitectural Load Port Data Sampling Firmware</a>	-	All	All	All
Operating System	<a href="#">Intel</a>	<a href="#">Microarchitectural Load Port Data Sampling Firmware</a>	-	All	All	All

## References

### Reference

- [Bugtraq: \[SECURITY\] \[DSA 4469-1\] libvirt security update](#)
- [\[SECURITY\] Fedora 29 Update: xen-4.11.1-5.fc29 - package-announce - Fedora Mailing-Lists](#)
- [Debian -- Security Information -- DSA-4602-1 xen](#)
- [FreeBSD-SA-19:26](#)
- [INTEL-SA-00233](#)
- [Red Hat Customer Portal](#)
- [\[security-announce\] openSUSE-SU-2019:1505-1: important: Security update](#)
- [Xen: Multiple vulnerabilities \(GLSA 202003-56\) — Gentoo security](#)

Synology Inc.

[www.arubanetworks.com/assets/alert/ARUBA-PSA-2019-003.txt](http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2019-003.txt)

McAfee Security Bulletin - Updates for Intel® "ZombieLoad" microprocessor data leakage flaws (CVE-2018-12126, CVE-2018-12127, CVE-20

[cert-portal.siemens.com/productcert/pdf/ssa-616472.pdf](http://cert-portal.siemens.com/productcert/pdf/ssa-616472.pdf)

[security-announce] openSUSE-SU-2019:1805-1: important: Security update

FreeBSD-SA-19:07

[SECURITY] [DLA 1789-2] intel-microcode security update

Bugtraq: FreeBSD Security Advisory FreeBSD-SA-19:26.mcu

[cert-portal.siemens.com/productcert/pdf/ssa-608355.pdf](http://cert-portal.siemens.com/productcert/pdf/ssa-608355.pdf)

USN-3977-3: Intel Microcode update | Ubuntu security notices

Bugtraq: [SECURITY] [DSA 4564-1] linux security update

FreeBSD Security Advisory - FreeBSD-SA-19:26.mcu ~ Packet Storm

Bugtraq: [SECURITY] [DSA 4602-1] xen security update

Security Advisory - Intel Microarchitectural Data Sampling (MDS) vulnerabilities

Bugtraq: [SECURITY] [DSA 4447-2] intel-microcode security update

Red Hat Customer Portal

[security-announce] openSUSE-SU-2019:1806-1: important: Security update

[SECURITY] Fedora 29 Update: xen-4.11.1-5.fc29 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[296079](#) Oracle Solaris 11.4 Support Repository Update (SRU) 15.5.0 Missing (CPUOCT2019)

[377003](#) Alibaba Cloud Linux Security Update for qemu-kvm (ALINUX2-SA-2019:0030)

[377032](#) Alibaba Cloud Linux Security Update for libvirt (ALINUX2-SA-2019:0032)

[378146](#) Virtuozzo Linux Security Update for libvirt-lock-sanlock (VZLSA-2019:1180)

[378208](#) Virtuozzo Linux Security Update for qemu-guest-agent (VZLSA-2019:1181)

[500752](#) Alpine Linux Security Update for xen

[504529](#) Alpine Linux Security Update for xen

[590937](#) Siemens SIMATIC WinAC RTX (F) 2010 Multiple Vulnerabilities (ssa-608355)

[591420](#) Siemens ZombieLoad and Microarchitectural Data Sampling Vulnerabilities (SSA-616472)

---

© [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](#)