



# CVE-2019-19580

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2019-19580   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2019-12-11 18:16:00 UTC  |
| <b>Updated</b>         | 2023-11-07 03:07:00 UTC  |
| <b>Description</b>     | An issue was discovered in Xen through 4.12.x allowing x86 PV guest OS users to gain host OS privileges by leveraging ra |

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a> | 31      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a> | 31      | All    | All     | All      |
| Operating System | <a href="#">Xen</a>           | <a href="#">Xen</a>    | All     | All    | All     | All      |

## References

| Reference  | Source  | Link   | Tags    |
|--|---------|--|---------|
| Debian -- Security Information -- DSA-4602-1 xen   | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>                   |         |
| Xen: Multiple vulnerabilities (GLSA 202003-56) — Gentoo security                         | GENTOO  | <a href="http://security.gentoo.org">security.gentoo.org</a>         |         |
| [SECURITY] Fedora 31 Update: xen-4.12.1-8.fc31 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> | Third F |
| [SECURITY] Fedora 30 Update: xen-4.11.3-2.fc30 - package-announce - Fedora Mailing-Lists | FEDORA  | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |         |
| [SECURITY] Fedora 31 Update: xen-4.12.1-8.fc31 - package-announce - Fedora Mailing-Lists |         | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |         |
| [security-announce] openSUSE-SU-2020:0011-1: important: Security update                  | SUSE    | <a href="http://lists.opensuse.org">lists.opensuse.org</a>           |         |
| XSA-310 - Xen Security Advisories  | MISC    | <a href="http://xenbits.xen.org">xenbits.xen.org</a>                 | Patch,  |
| Bugtraq: [SECURITY] [DSA 4602-1] xen security update                                     | BUGTRAQ | <a href="http://seclists.org">seclists.org</a>                       |         |
| [SECURITY] Fedora 30 Update: xen-4.11.3-2.fc30 - package-announce - Fedora Mailing-Lists |         | <a href="http://lists.fedoraproject.org">lists.fedoraproject.org</a> |         |
| CVE Program record   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                         | canoni  |
| NVD vulnerability detail   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                       | canoni  |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

378871 Citrix XenServer Security Updates (CTX266932)

500754 Alpine Linux Security Update for xen

504531 Alpine Linux Security Update for xen

© [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](#).

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