



CVE-2020-7059

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2020-7059 |
| State | PUBLIC |
| Assigner | security@php.net |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-02-10 08:15:00 UTC |
| Updated | 2022-07-01 12:42:00 UTC |
| Description | When using fgetss() function to read data with stripping tags, in PHP versions 7.2.x below 7.2.27, 7.3.x below 7.3.14 and 7. |

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------|--|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Opensuse | Leap | 15.1 | All | All | All |
| Application | Oracle | Communications Diameter Signaling Router | All | All | All | All |
| Application | Php | Php | All | All | All | All |
| Application | Php | Php | All | All | All | All |
| Application | Tenable | Tenable.sc | All | All | All | All |

References

| Reference | Source | Link | Tags |
|--|---------|-------------------------------------|----------|
| PHP :: Sec Bug #79099 :: OOB read in php_strip_tags_ex | MISC | bugs.php.net | Exploit, |
| [SECURITY] [DLA 2124-1] php5 security update | MLIST | lists.debian.org | |
| Bugtraq: [SECURITY] [DSA 4626-1] php7.3 security update | BUGTRAQ | seclists.org | |
| Oracle Critical Patch Update Advisory - July 2020 | MISC | www.oracle.com | |
| [security-announce] openSUSE-SU-2020:0341-1: important: Security update | SUSE | lists.opensuse.org | |
| PHP: Multiple vulnerabilities (GLSA 202003-57) — Gentoo security | GENTOO | security.gentoo.org | |
| [R1] Tenable.sc 5.19.0 Fixes Multiple Third-party Vulnerabilities - Security Advisory Tenable® | CONFIRM | www.tenable.com | |
| Debian -- Security Information -- DSA-4628-1 php7.0 | DEBIAN | www.debian.org | |

| | | | |
|--|---------|--|---------|
| Debian -- Security Information -- DSA-4626-1 php7.3 | DEBIAN | www.debian.org | |
| Bugtraq: Re: [SECURITY] [DSA 4628-1] php7.0 security update | BUGTRAQ | seclists.org | |
| February 2020 PHP Vulnerabilities in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com | |
| USN-4279-1: PHP vulnerabilities Ubuntu security notices | UBUNTU | usn.ubuntu.com | |
| Bugtraq: [SECURITY] [DSA 4628-1] php7.0 security update | BUGTRAQ | seclists.org | |
| Oracle Critical Patch Update Advisory - April 2021 | MISC | www.oracle.com | |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

Vendor Comments And Credit

Discovery Credit

LEGACY: Reported by wxhusst at gmail dot com

Legacy QID Mappings

[296076](#) Oracle Solaris 11.4 Support Repository Update (SRU) 19.3.0 Missing (CPUJAN2020)

[501135](#) Alpine Linux Security Update for php7

[752878](#) SUSE Enterprise Linux Security Update for php7 (SUSE-SU-2022:4067-1)

[940250](#) AlmaLinux Security Update for php:7.3 (ALSA-2020:3662)

[960421](#) Rocky Linux Security Update for php:7.3 (RLSA-2020:3662)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report