



# CVE-2016-5385

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

## Summary

<b>CVE</b>	CVE-2016-5385
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-07-19 02:00:00 UTC
<b>Updated</b>	2023-02-12 23:23:00 UTC
<b>Description</b>	PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not prote

## Risk And Classification

**Problem Types:** CWE-601

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Drupal</a>	<a href="#">Drupal</a>	All	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	23	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	24	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storeever Msl6480 Tape Library</a>	-	All	All	All
Hardware	<a href="#">Hp</a>	<a href="#">Storeever Msl6480 Tape Library</a>	-	All	All	All
Operating System	<a href="#">Hp</a>	<a href="#">Storeever Msl6480 Tape Library Firmware</a>	All	All	All	All
Application	<a href="#">Hp</a>	<a href="#">System Management Homepage</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications User Data Repository</a>	10.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications User Data Repository</a>	10.0.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications User Data Repository</a>	12.0.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Enterprise Manager Ops Center</a>	12.2.2	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Enterprise Manager Ops Center</a>	12.3.2	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	6	-	All	All

Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	7	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	7	-	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	7	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	All	All	All	All
Application	<a href="#">Php</a>	<a href="#">Php</a>	All	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All

## References

### Reference

[SECURITY] Fedora 24 Update: php-guzzlehttp-guzzle6-6.2.1-1.fc24 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 24 Update: php-guzzlehttp-guzzle6-6.2.1-1.fc24 - package-announce - Fedora Mailing-Lists

openSUSE-SU-2016:1922-1: moderate: Security update for php5

[SECURITY] Fedora 24 Update: php-5.6.24-2.fc24 - package-announce - Fedora Mailing-Lists

Vulnerability Note VU#797896 - CGI web servers assign Proxy header values from client requests to internal HTTP\_PROXY environment vari

Document Display | HPE Support Center

Red Hat Customer Portal

httproxy

Oracle Critical Patch Update - January 2018

Oracle Linux Bulletin - July 2016

Document Display | HPE Support Center

Red Hat Customer Portal

Release 6.2.1 release · guzzle/guzzle · GitHub

Red Hat Customer Portal

CVE-2016-5385 - Red Hat Customer Portal

Red Hat Customer Portal

Red Hat Customer Portal

Debian -- Security Information -- DSA-3631-1 php5

Red Hat Customer Portal

Bug 1353794 – CVE-2016-5385 PHP: sets environmental variable based on user supplied Proxy request header

[SECURITY] Fedora 24 Update: php-5.6.24-2.fc24 - package-announce - Fedora Mailing-Lists

Red Hat Customer Portal
Document Display   HPE Support Center
Red Hat Customer Portal
Red Hat Customer Portal
[SECURITY] Fedora 23 Update: php-guzzlehttp-guzzle6-6.2.1-1.fc23 - package-announce - Fedora Mailing-Lists
PHP CVE-2016-5385 Security Bypass Vulnerability
Drupal Core - Highly Critical - Injection - SA-CORE-2016-003   Drupal.org
Document Display   HPE Support Center
PHP "Proxy:" Header Processing Flaw Lets Remote Users Redirect the Target Application Requests to an Arbitrary Web Proxy in Certain Cas
Red Hat Customer Portal
Oracle Critical Patch Update - July 2017
PHP: Multiple vulnerabilities (GLSA 201611-22) — Gentoo security
[SECURITY] Fedora 23 Update: php-guzzlehttp-guzzle6-6.2.1-1.fc23 - package-announce - Fedora Mailing-Lists
CVE Program record
NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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

© [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](https://www.mitre.org/licenses/mitre).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**