# CVE-2014-4049

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2014-4049 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2014-06-18 19:55:00 UTC |
| **Updated** | 2022-08-29 20:05:00 UTC |
| **Description** | Heap-based buffer overflow in the php_parserr function in ext/standard/dns.c in PHP 5.6.0beta4 and earlier allows remote s |

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 7.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Opensuse | Opensuse | 11.3 | All | All | All |
| Operating System | Opensuse | Opensuse | 11.3 | All | All | All |
| Application | Php | Php | All | All | All | All |
| Application | Php | Php | 5.6.0 | alpha1 | All | All |
| Application | Php | Php | 5.6.0 | alpha2 | All | All |
| Application | Php | Php | 5.6.0 | alpha3 | All | All |
| Application | Php | Php | 5.6.0 | alpha4 | All | All |
| Application | Php | Php | 5.6.0 | alpha5 | All | All |
| Application | Php | Php | 5.6.0 | beta1 | All | All |
| Application | Php | Php | 5.6.0 | beta2 | All | All |
| Application | Php | Php | 5.6.0 | beta3 | All | All |
| Application | Php | Php | 5.6.0 | alpha1 | All | All |
| Application | Php | Php | 5.6.0 | alpha2 | All | All |
| Application | Php | Php | 5.6.0 | alpha3 | All | All |
| Application | Php | Php | 5.6.0 | alpha4 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Php | Php | 5.6.0 | alpha5 | All | All |
| Application | Php | Php | 5.6.0 | beta1 | All | All |
| Application | Php | Php | 5.6.0 | beta2 | All | All |
| Application | Php | Php | 5.6.0 | beta3 | All | All |
| Application | Php | Php | All | beta4 | All | All |

## References

| Reference |
|---|
| Oracle Bulletin Board Update - January 2015 |
| Red Hat Customer Portal |
| About Secunia Research \| Flexera |
| About the security content of OS X Mavericks v10.9.5 and Security Update 2014-004 - Apple Support |
| About Secunia Research \| Flexera |
| '[security bulletin] HPSBUX03102 SSRT101681 rev.1 - HP-UX Apache Server Suite running Apache Tomcat o' - MARC |
| oss-security - Re: CVE request: PHP heap-based buffer overflow in DNS TXT record parsing |
| Merge branch 'PHP-5.6' · php/php-src@b34d784 · GitHub |
| APPLE-SA-2015-04-08-2 OS X 10.10.3 and Security Update 2015-004 |
| Debian -- Security Information -- DSA-2961-1 php5 |
| Security Advisory SA59329 - Ubuntu update for php5 - Secunia |
| About Secunia Research \| Flexera |
| [security-announce] SUSE-SU-2014:0868-1: important: Security update for |
| openSUSE-SU-2014:0841-1: moderate: php5: Update to prevent insecure DNS |
| PHP DNS TXT Record Handling Heap Buffer Overflow Vulnerability |
| Security Advisory SA59513 - SUSE update for php5 - Secunia |
| Security Advisory SA59652 - SUSE update for php5 - Secunia |
| PHP Buffer Overflow in dns_get_record() Lets Remote Users Execute Arbitrary Code - SecurityTracker |
| [security-announce] SUSE-SU-2014:0869-1: important: Security update for |
| Red Hat Customer Portal |
| IBM Security Bulletin: Multiple vulnerabilities in PHP 5.2 open source component for IBM Lotus Protector for Mail Security (CVE-2014-3515 CV |
| Security Advisory SA60998 - IBM Lotus Protector for Mail Security PHP Multiple Vulnerabilities - Secunia |
| About the security content of OS X Yosemite v10.10.3 and Security Update 2015-004 - Apple Support |
| Bug 1108447 – CVE-2014-4049 php: heap-based buffer overflow in DNS TXT record parsing |
| openSUSE-SU-2014:0942-1: moderate: Update to prevent insecure DNS TXT re |
| 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.



**Free CVE JSON API** cve.report/api

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