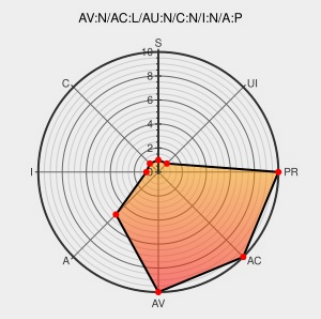
# CVE-2011-4153

Published on: 01/18/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:11 PM UTC

## CVE-2011-4153

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Php from Php contain the following vulnerability:

PHP 5.3.8 does not always check the return value of the zend_strndup function, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted input to an application that performs strndup operations on untrusted string data, as demonstrated by the define function in zend_builtin_functions.c, and unspecified functions in ext/soap/php_sdl.c, ext/standard/syslog.c, ext/standard/browscap.c, ext/oci8/oci8.c, ext/com_dotnet/com_typeinfo.c, and main/php_open_temporary_file.c.

CVE-2011-4153 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| HPSBMU02786 SSRT100877 rev.2 - HP System Management Homepage (SMH) Running on Linux, Windows, and VMware ESX, Remote Unauthorized Access, Disclosure of Information, Data Modification, Denial of Service (DoS), Execution of Arbitrary Code - c03360041 - HP Business Support Center | web.archive.org text/html Inactive Link Not Archived | HP HPSBMU02786 |
| [security-announce] SUSE-SU-2012:0411-1: important: Security update for | lists.opensuse.org text/html | SUSE SUSE-SU-2012:0411 |
| Security Alerts - Secunia | web.archive.org text/html | SECUNIA 48668 |
| [security-announce] openSUSE-SU-2012:0426-1: important: update for php5 | lists.opensuse.org | SUSE openSUSE-SU- |

| | | |
|---|---|---|
| | text/html | 2012:0426 |
| NEOHAPSIS - Peace of Mind Through Integrity and Insight | Exploit<br>web.archive.org<br>text/html<br>Inactive Link Not Archived | BUGTRAQ 20120114 PHP 5.3.8 Multiple vulnerabilities |
| PHP 5.3.8 Multiple Vulnerabilities | Exploit<br>www.exploit-db.com<br>Proof of Concept<br>text/html | EXPLOIT-DB 18370 |
| [security-announce] SUSE-SU-2012:0472-1: important: Security update for | lists.opensuse.org<br>text/html | SUSE SUSE-SU-2012:0472 |
| CXResearch PHP 5.3.8 Multiple vulnerabilities - CXSecurity Research WLB2 | Exploit<br>cxsecurity.com<br>text/html | MISC cxsecurity.com/research/103 |
| '[security bulletin] HPSBUX02791 SSRT100856 rev.1 - HP-UX Apache Web Server running PHP, Remote Execu' - MARC | marc.info<br>text/html | HP SSRT100856 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Php | Php | 5.3.8 | All | All | All |
| Application | Php | Php | 5.3.8 | All | All | All |

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*

cpe:2.3:a:php:php:5.3.8:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
|---|---|---|
| /r/Fedora | Is my Fedora Workstation infected? Test results from Chrootkit, rkhunter, clamscan posted. Help! | 2018-06-25 02:42:39 |

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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**