



# CVE-2017-11362

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

## Summary

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-11362                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                       |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                 |
| <b>Published</b>       | 2017-07-17 13:18:00 UTC                                                                                                      |
| <b>Updated</b>         | 2019-05-22 16:29:00 UTC                                                                                                      |
| <b>Description</b>     | In PHP 7.x before 7.0.21 and 7.1.x before 7.1.7, ext/intl/msgformat/msgformat_parse.c does not restrict the locale length, w |

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|---------|---------|--------|---------|----------|
| Application | Php    | Php     | 7.0.0   | All    | All     | All      |
| Application | Php    | Php     | 7.0.1   | All    | All     | All      |
| Application | Php    | Php     | 7.0.10  | All    | All     | All      |
| Application | Php    | Php     | 7.0.11  | All    | All     | All      |
| Application | Php    | Php     | 7.0.12  | All    | All     | All      |
| Application | Php    | Php     | 7.0.13  | All    | All     | All      |
| Application | Php    | Php     | 7.0.14  | All    | All     | All      |
| Application | Php    | Php     | 7.0.15  | All    | All     | All      |
| Application | Php    | Php     | 7.0.16  | All    | All     | All      |
| Application | Php    | Php     | 7.0.17  | All    | All     | All      |
| Application | Php    | Php     | 7.0.18  | All    | All     | All      |
| Application | Php    | Php     | 7.0.19  | All    | All     | All      |
| Application | Php    | Php     | 7.0.2   | All    | All     | All      |
| Application | Php    | Php     | 7.0.20  | All    | All     | All      |
| Application | Php    | Php     | 7.0.3   | All    | All     | All      |
| Application | Php    | Php     | 7.0.4   | All    | All     | All      |
| Application | Php    | Php     | 7.0.5   | All    | All     | All      |

|             |     |     |        |     |     |     |
|-------------|-----|-----|--------|-----|-----|-----|
|             |     |     |        |     |     |     |
| Application | Php | Php | 7.0.6  | All | All | All |
| Application | Php | Php | 7.0.7  | All | All | All |
| Application | Php | Php | 7.0.8  | All | All | All |
| Application | Php | Php | 7.0.9  | All | All | All |
| Application | Php | Php | 7.1.0  | All | All | All |
| Application | Php | Php | 7.1.1  | All | All | All |
| Application | Php | Php | 7.1.2  | All | All | All |
| Application | Php | Php | 7.1.3  | All | All | All |
| Application | Php | Php | 7.1.4  | All | All | All |
| Application | Php | Php | 7.1.5  | All | All | All |
| Application | Php | Php | 7.1.6  | All | All | All |
| Application | Php | Php | 7.0.0  | All | All | All |
| Application | Php | Php | 7.0.1  | All | All | All |
| Application | Php | Php | 7.0.10 | All | All | All |
| Application | Php | Php | 7.0.11 | All | All | All |
| Application | Php | Php | 7.0.12 | All | All | All |
| Application | Php | Php | 7.0.13 | All | All | All |
| Application | Php | Php | 7.0.14 | All | All | All |
| Application | Php | Php | 7.0.15 | All | All | All |
| Application | Php | Php | 7.0.16 | All | All | All |
| Application | Php | Php | 7.0.17 | All | All | All |
| Application | Php | Php | 7.0.18 | All | All | All |
| Application | Php | Php | 7.0.19 | All | All | All |
| Application | Php | Php | 7.0.2  | All | All | All |
| Application | Php | Php | 7.0.20 | All | All | All |
| Application | Php | Php | 7.0.3  | All | All | All |
| Application | Php | Php | 7.0.4  | All | All | All |
| Application | Php | Php | 7.0.5  | All | All | All |
| Application | Php | Php | 7.0.6  | All | All | All |
| Application | Php | Php | 7.0.7  | All | All | All |
| Application | Php | Php | 7.0.8  | All | All | All |
| Application | Php | Php | 7.0.9  | All | All | All |
| Application | Php | Php | 7.1.0  | All | All | All |
| Application | Php | Php | 7.1.1  | All | All | All |
| Application | Php | Php | 7.1.2  | All | All | All |

|             |     |     |       |     |     |     |
|-------------|-----|-----|-------|-----|-----|-----|
| Application | Php | Php | 7.1.3 | All | All | All |
| Application | Php | Php | 7.1.4 | All | All | All |
| Application | Php | Php | 7.1.5 | All | All | All |
| Application | Php | Php | 7.1.6 | All | All | All |

| References                                                                      |         |  |                                                               |                     |  |  |
|---------------------------------------------------------------------------------|---------|--|---------------------------------------------------------------|---------------------|--|--|
| Reference                                                                       | Source  |  | Link                                                          | Tags                |  |  |
| PHP: Multiple vulnerabilities (GLSA 201709-21) — Gentoo security                | GENTOO  |  | <a href="https://security.gentoo.org">security.gentoo.org</a> |                     |  |  |
| PHP :: Bug #73473 :: Stack Buffer Overflow in msgfmt_parse_message              | MISC    |  | <a href="https://bugs.php.net">bugs.php.net</a>               | Issue Tracking, Ver |  |  |
| Red Hat Customer Portal                                                         | REDHAT  |  | <a href="https://access.redhat.com">access.redhat.com</a>     |                     |  |  |
| USN-3566-2: PHP vulnerabilities   Ubuntu security notices                       | UBUNTU  |  | <a href="https://usn.ubuntu.com">usn.ubuntu.com</a>           |                     |  |  |
| September 2017 PHP Vulnerabilities in NetApp Products   NetApp Product Security | CONFIRM |  | <a href="https://security.netapp.com">security.netapp.com</a> |                     |  |  |
| CVE Program record                                                              | CVE.ORG |  | <a href="https://www.cve.org">www.cve.org</a>                 | canonical           |  |  |
| NVD vulnerability detail                                                        | NVD     |  | <a href="https://nvd.nist.gov">nvd.nist.gov</a>               | canonical, analysis |  |  |

No vendor comments have been submitted for this CVE.

| Legacy QID Mappings                                                                        |  |  |  |  |  |  |
|--------------------------------------------------------------------------------------------|--|--|--|--|--|--|
| 710414 Gentoo Linux Hypertext Preprocessor (PHP) Multiple Vulnerabilities (GLSA 201709-21) |  |  |  |  |  |  |

© [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). This site includes MITRE data granted under the following [license](https://www.mitre.org).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

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