CVE-2016-9935

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

Summary

CVE	CVE-2016-9935
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-04 20:59:00 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attack

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.043930000 probability, percentile 0.890610000 (date 2026-05-10)

Problem Types: CWE-125 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

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	7.0.2	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	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
PHP: Multiple vulnerabilities (GLSA 201702-29) — Gentoo Security	af854a3a-2127-422b-91ae-364
openSUSE-SU-2017:0081-1: moderate: Security update for php5	af854a3a-2127-422b-91ae-364
Debian -- Security Information -- DSA-3737-1 php5	af854a3a-2127-422b-91ae-364
PHP: PHP 5 ChangeLog	af854a3a-2127-422b-91ae-364
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364
oss-security - CVE assignment for PHP 5.6.28, 5.6.29, 7.0.13, 7.0.14 and 7.1.0	af854a3a-2127-422b-91ae-364
PHP: PHP 7 ChangeLog	af854a3a-2127-422b-91ae-364
PHP 'ext/wddx/wddx.c' Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364
openSUSE-SU-2017:0061-1: moderate: Security update for php7	af854a3a-2127-422b-91ae-364
Fix bug #73631 - Invalid read when wddx decodes empty boolean element · php/php-src@66fd442 · GitHub	af854a3a-2127-422b-91ae-364
openSUSE-SU-2016:3239-1: moderate: Security update for php5	af854a3a-2127-422b-91ae-364
PHP :: Sec Bug #73631 :: Invalid read when wddx decodes empty boolean element	af854a3a-2127-422b-91ae-364
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

710436 Gentoo Linux Hypertext Preprocessor (PHP) Multiple Vulnerabilities (GLSA 201702-29)