



CVE-2015-6838

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

Summary

CVE	CVE-2015-6838
State	PUBLIC
Assigner	security@microfocus.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-16 10:59:00 UTC
Updated	2023-11-07 02:27:00 UTC
Description	The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php	Php	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All
Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All
Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All
Application	Php	Php	5.5.12	All	All	All

Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.14	All	All	All
Application	Php	Php	5.5.15	All	All	All
Application	Php	Php	5.5.16	All	All	All
Application	Php	Php	5.5.17	All	All	All
Application	Php	Php	5.5.18	All	All	All
Application	Php	Php	5.5.19	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.20	All	All	All
Application	Php	Php	5.5.21	All	All	All
Application	Php	Php	5.5.22	All	All	All
Application	Php	Php	5.5.23	All	All	All
Application	Php	Php	5.5.24	All	All	All
Application	Php	Php	5.5.25	All	All	All
Application	Php	Php	5.5.26	All	All	All
Application	Php	Php	5.5.27	All	All	All
Application	Php	Php	5.5.28	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	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	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All

Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All
Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	5.5.0	All	All	All
Application	Php	Php	5.5.0	alpha1	All	All
Application	Php	Php	5.5.0	alpha2	All	All
Application	Php	Php	5.5.0	alpha3	All	All
Application	Php	Php	5.5.0	alpha4	All	All
Application	Php	Php	5.5.0	alpha5	All	All
Application	Php	Php	5.5.0	alpha6	All	All
Application	Php	Php	5.5.0	beta1	All	All
Application	Php	Php	5.5.0	beta2	All	All
Application	Php	Php	5.5.0	beta3	All	All
Application	Php	Php	5.5.0	beta4	All	All
Application	Php	Php	5.5.0	rc1	All	All
Application	Php	Php	5.5.0	rc2	All	All
Application	Php	Php	5.5.1	All	All	All
Application	Php	Php	5.5.10	All	All	All
Application	Php	Php	5.5.11	All	All	All
Application	Php	Php	5.5.12	All	All	All
Application	Php	Php	5.5.13	All	All	All
Application	Php	Php	5.5.14	All	All	All
Application	Php	Php	5.5.15	All	All	All
Application	Php	Php	5.5.16	All	All	All
Application	Php	Php	5.5.17	All	All	All
Application	Php	Php	5.5.18	All	All	All
Application	Php	Php	5.5.19	All	All	All
Application	Php	Php	5.5.2	All	All	All
Application	Php	Php	5.5.20	All	All	All

Application	Php	Php	5.5.20	All	All	All
Application	Php	Php	5.5.21	All	All	All
Application	Php	Php	5.5.22	All	All	All
Application	Php	Php	5.5.23	All	All	All
Application	Php	Php	5.5.24	All	All	All
Application	Php	Php	5.5.25	All	All	All
Application	Php	Php	5.5.26	All	All	All
Application	Php	Php	5.5.27	All	All	All
Application	Php	Php	5.5.28	All	All	All
Application	Php	Php	5.5.3	All	All	All
Application	Php	Php	5.5.4	All	All	All
Application	Php	Php	5.5.5	All	All	All
Application	Php	Php	5.5.6	All	All	All
Application	Php	Php	5.5.7	All	All	All
Application	Php	Php	5.5.8	All	All	All
Application	Php	Php	5.5.9	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	beta4	All	All
Application	Php	Php	5.6.1	All	All	All
Application	Php	Php	5.6.10	All	All	All
Application	Php	Php	5.6.11	All	All	All
Application	Php	Php	5.6.12	All	All	All
Application	Php	Php	5.6.2	All	All	All
Application	Php	Php	5.6.3	All	All	All
Application	Php	Php	5.6.4	All	All	All
Application	Php	Php	5.6.5	All	All	All
Application	Php	Php	5.6.6	All	All	All
Application	Php	Php	5.6.7	All	All	All
Application	Php	Php	5.6.8	All	All	All

Application	Php	Php	5.6.9	All	All	All
Application	Php	Php	All	All	All	All
Application	Xmlsoft	Libxml2	All	All	All	All

References

Reference	Source
PHP Multiple Bugs Let Remote Users Obtain Potentially Sensitive Information, View Files, and Execute Arbitrary Code - SecurityTracker	SE
PHP 'xsltprocessor.c' Null Pointer Deference Denial of Service Vulnerability	BL
PHP: Multiple vulnerabilities (GLSA 201606-10) — Gentoo security	GE
PHP: PHP 5 ChangeLog	CC
Debian -- Security Information -- DSA-3358-1 php5	
PHP :: Sec Bug #69782 :: NULL pointer dereference	CC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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