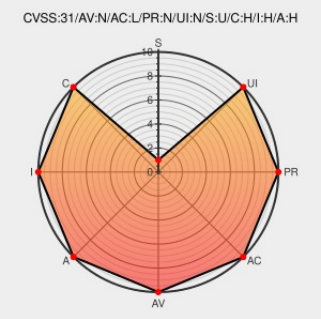
CVE-2017-5340

Published on: 01/11/2017 12:00:00 AM UTC

Last Modified on: 07/20/2022 04:46:00 PM UTC

CVE-2017-5340

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



Certain versions of Clustered Data Ontap from Netapp contain the following vulnerability:

Zend/zend_hash.c in PHP before 7.0.15 and 7.1.x before 7.1.1 mishandles certain cases that require large array allocations, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow, uninitialized memory access, and use of arbitrary destructor function pointers) via crafted serialized data.

CVE-2017-5340 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
PHP :: Sec Bug #73832 :: Use of uninitialized memory in unserialize()	Exploit VDB Entry bugs.php.net	CONFIRM bugs.php.net/bug.php?id=73832

	text/html	
PHP CVE-2017-5340 Remote Code Execution Vulnerability	cve.report (archive) text/html	BID 95371
Red Hat Customer Portal	access.redhat.com text/html	REDHAT RHSA-2018:1296
PHP Multiple Flaws Let Remote and Local Users Obtain Potentially Sensitive Information, Deny Service, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1037659
Fix #73832 - leave the table in a safe state if the size is too big. · php/php-src@4cc0286 · GitHub	VDB Entry github.com text/html	CONFIRM github.com/php/php-src/commit/4cc0286f2f3780abc6084bcdae5dce595daa3c12
September 2017 PHP Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20180112-0001/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Clustered Data Ontap	-	All	All	All
Application	Php	Php	All	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	7.0.2	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	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	7.0.2	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

cpe:2.3:a:netapp:clustered_data_ontap:-:*:*:*:*:*:*:*:

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

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.11:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.12:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.14:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.7:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:7.0.0:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.1:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.10:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.11:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.12:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.13:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.14:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.2:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.3:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.4:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.5:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.6:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.7:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.8:*:*:*:*:*:*:*

cpe:2.3:a:php:php:7.0.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→