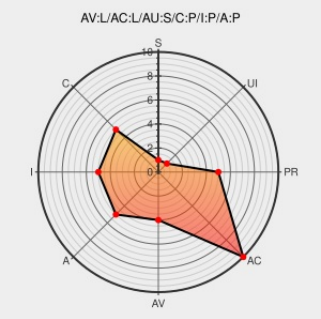
CVE-2007-1710

Published on: 03/26/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:37 PM UTC

CVE-2007-1710

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



Certain versions of Php from Php contain the following vulnerability:

The readfile function in PHP 4.4.4, 5.1.6, and 5.2.1 allows context-dependent attackers to bypass safe_mode restrictions and read arbitrary files by referring to local files with a certain URL syntax instead of a pathname syntax, as demonstrated by a filename preceded a "php://../../" sequence.

CVE-2007-1710 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
HPSBMA02215 SSRT071423 rev.1 - HP System Management Homepage (SMH) for Linux and Windows Running PHP, Remote Execution of Arbitrary Code - c01056506 - HP Business Support Center	web.archive.org text/html Inactive Link Not Archived	HP SSRT071423
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2007-1991
HPSBTU02232 SSRT071429 rev.1 - Secure Web Server for HP Tru64 UNIX Powered by Apache (SWS) or HP Internet Express for Tru64 UNIX running PHP, Remote Arbitrary Code Execution, Unauthorized Disclosure of Information, or Denial of Service (DoS) - c01086137 - HP Business Support Center	web.archive.org text/html Inactive Link Not Archived	HP HPSBTU02232
HP System Management Homepage PHP Multiple Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 25423
404 Page Not Found | Exploit Database	www.exploit-db.com	EXPLOIT-

	Proof of Concept text/html Inactive Link Not Archived	DB 3573
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2007-2374
HP Secure Web Server/Internet Express for Tru64 UNIX PHP Vulnerabilities - Advisories - Secunia	web.archive.org text/html	SECUNIA 25850

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	4.4.4	All	All	All
Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.1	All	All	All
Application	Php	Php	4.4.4	All	All	All
Application	Php	Php	5.1.6	All	All	All
Application	Php	Php	5.2.1	All	All	All

cpe:2.3:a:php:php:4.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:4.4.4:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:php:php:5.2.1:*:*:*:*:*:*:*:

← Previous ID

Next ID→

© CVE.report 2023 |
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 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