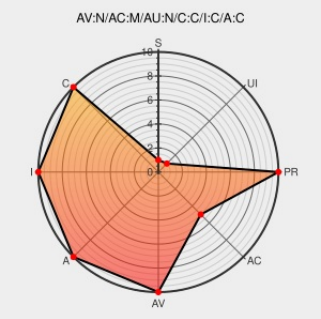
CVE-2007-5653

Published on: 10/23/2007 12:00:00 AM UTC

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

CVE-2007-5653

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



Certain versions of Php from Php contain the following vulnerability:

The Component Object Model (COM) functions in PHP 5.x on Windows do not follow safe_mode and disable_functions restrictions, which allows context-dependent attackers to bypass intended limitations, as demonstrated by executing objects with the kill bit set in the corresponding ActiveX control Compatibility Flags, executing programs via a function in compatUI.dll, invoking wscript.shell via wscript.exe, invoking Scripting.FileSystemObject via wshom.ocx, and adding users via a function in shgina.dll, related to the com_load_typelib function.

CVE-2007-5653 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF php-com-security-bypass(37368)
PHP COM Objects Security Bypass - Advisories - Secunia	web.archive.org text/html	SECUNIA 27280
PHP 5.x COM functions safe_mode and disable_function bypass	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 4553
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2007-3590

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	All	All	windows	All

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

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report