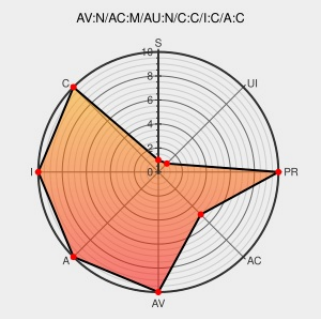
CVE-2004-1875

Published on: 03/30/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1875

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



Certain versions of Cpanel from Cpanel contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in cPanel 9.1.0-R85 allow remote attackers to inject arbitrary web script or HTML via the (1) email parameter to testfile.html, (2) file parameter to erredit.html, (3) dns parameter to dnslook.html, (4) account parameter to ignorelist.html, (5) account parameter to showlog.html, (6) db parameter to repairdb.html, (7) login parameter to doaddftp.html (8) account parameter to editmsg.htm, or (9) ip parameter to del.html. NOTE: the dnslook.html vector was later reported to exist in cPanel 10.

CVE-2004-1875 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
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4243
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4212
		MISC www.aria

	www.ara-security.com text/plain Inactive Link Not Archived	MISC www.ara-security.com/forum/showthread.php?t=30
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4210
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4208
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2006-4658
cPanel Cross Site Scripting (XSS)	Patch Vendor Advisory web.archive.org text/html Inactive Link Not Archived	MISC www.cirt.net/advisories/cpanel_xss.shtml
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4209
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4213
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 4211
CPanel DNSlook.HTML Cross-Site Scripting Vulnerability	cve.report (archive) text/html	BID 21142
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4214
cPanel Multiple Module Cross-Site Scripting Vulnerabilities	Vendor Advisory cve.report (archive) text/html	BID 10002
'Exensive cPanel Cross Site Scripting' - MARC	marc.info text/html	BUGTRAQ 20040330 Exensive cPanel Cross Site Scripting
cPanel "dns" Cross-Site Scripting Vulnerability - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 22984
No Description Provided	Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 4215
Secunia - Advisories - cPanel Multiple Cross-Site Scripting Vulnerabilities	Patch Vendor Advisory web.archive.org text/html	SECUNIA 11244
IBM X-Force Exchange	exchange.xforce.ibmcloud.com	XF cpanel-multiple-scripts-xss(15671)

text/html

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	Cpanel	Cpanel	9.1.0_r85	All	All	All
Application	Cpanel	Cpanel	9.1.0_r85	All	All	All

cpe:2.3:a:cpanel:cpanel:9.1.0_r85:*:*:*:*:*:*:*:

cpe:2.3:a:cpanel:cpanel:9.1.0_r85:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→