



CVE-2004-1769

Published on: 03/11/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1769

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Cpanel](#) from [Cpanel](#) contain the following vulnerability:

The "Allow cPanel users to reset their password via email" feature in cPanel 9.1.0 build 34 and earlier, including 8.x, allows remote attackers to execute arbitrary code via the user parameter to resetpass.

CVE-2004-1769 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Secunia - Advisories - cPanel Password Reset Command Injection Vulnerability

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X SECUNIA 11111](#)

'cPanel Security Advisory CPANEL-2004:01-01' - MARC

[marc.info](#)
[text/html](#)

[BUGTRAQ 20040311 cPanel Security Advisory CPANEL-2004:01-01](#)

SecurityFocus

[Vendor Advisory](#)
[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20040311 Cpanel 8.*.* have a problem ?](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF cpanel-resetpass-execute-commands\(15443\)](#)

VU#831534 - cPanel fails to verify input passed to the "user" parameter

[Third Party Advisory](#)
[US Government Resource](#)
[www.kb.cert.org](#)

[CERT-VN VU#831534](#)

[text/html](#)

cPanel Resetpass Remote Command Execution Vulnerability

[Exploit](#)[🌐 BID 9848](#)[Vendor Advisory](#)[cve.report \(archive\)](#)[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

Exploit/POC from Github

CVE-2004-1769 // Mass cPanel Reset password

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cpanel	Cpanel	5.0	All	All	All
Application	Cpanel	Cpanel	5.3	All	All	All
Application	Cpanel	Cpanel	6.0	All	All	All
Application	Cpanel	Cpanel	6.2	All	All	All
Application	Cpanel	Cpanel	6.4	All	All	All
Application	Cpanel	Cpanel	6.4.1	All	All	All
Application	Cpanel	Cpanel	6.4.2	All	All	All
Application	Cpanel	Cpanel	6.4.2_stable_48	All	All	All
Application	Cpanel	Cpanel	7.0	All	All	All
Application	Cpanel	Cpanel	8.0	All	All	All
Application	Cpanel	Cpanel	9.0	All	All	All
Application	Cpanel	Cpanel	9.1	All	All	All
Application	Cpanel	Cpanel	5.0	All	All	All
Application	Cpanel	Cpanel	5.3	All	All	All
Application	Cpanel	Cpanel	6.0	All	All	All
Application	Cpanel	Cpanel	6.2	All	All	All
Application	Cpanel	Cpanel	6.4	All	All	All
Application	Cpanel	Cpanel	6.4.1	All	All	All
Application	Cpanel	Cpanel	6.4.2	All	All	All
Application	Cpanel	Cpanel	6.4.2_stable_48	All	All	All
Application	Cpanel	Cpanel	7.0	All	All	All

Application	Cpanel	Cpanel	8.0	All	All	All
Application	Cpanel	Cpanel	9.0	All	All	All
Application	Cpanel	Cpanel	9.1	All	All	All
cpe:2.3:a:cpanel:cpanel:5.0:*****:						
cpe:2.3:a:cpanel:cpanel:5.3:*****:						
cpe:2.3:a:cpanel:cpanel:6.0:*****:						
cpe:2.3:a:cpanel:cpanel:6.2:*****:						
cpe:2.3:a:cpanel:cpanel:6.4:*****:						
cpe:2.3:a:cpanel:cpanel:6.4.1:*****:						
cpe:2.3:a:cpanel:cpanel:6.4.2:*****:						
cpe:2.3:a:cpanel:cpanel:6.4.2_stable_48:*****:						
cpe:2.3:a:cpanel:cpanel:7.0:*****:						
cpe:2.3:a:cpanel:cpanel:8.0:*****:						
cpe:2.3:a:cpanel:cpanel:9.0:*****:						
cpe:2.3:a:cpanel:cpanel:9.1:*****:						
cpe:2.3:a:cpanel:cpanel:5.0:*****:						
cpe:2.3:a:cpanel:cpanel:5.3:*****:						
cpe:2.3:a:cpanel:cpanel:6.0:*****:						
cpe:2.3:a:cpanel:cpanel:6.2:*****:						
cpe:2.3:a:cpanel:cpanel:6.4:*****:						
cpe:2.3:a:cpanel:cpanel:6.4.1:*****:						
cpe:2.3:a:cpanel:cpanel:6.4.2:*****:						
cpe:2.3:a:cpanel:cpanel:6.4.2_stable_48:*****:						
cpe:2.3:a:cpanel:cpanel:7.0:*****:						
cpe:2.3:a:cpanel:cpanel:8.0:*****:						
cpe:2.3:a:cpanel:cpanel:9.0:*****:						
cpe:2.3:a:cpanel:cpanel:9.1:*****:						

No vendor comments have been submitted for this CVE

© [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 registered 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](#)