



CVE-2012-3953

Published on: 08/11/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:16 PM UTC

CVE-2012-3953

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

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

SQL injection vulnerability in admin/index.php in phpList before 2.10.19 allows remote administrators to execute arbitrary SQL commands via the delete parameter to the editattributes page.

CVE-2012-3953 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

File Not Found

[Exploit](#)
[www.htbridge.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[MISC](#) [www.htbridge.com/advisory/HTB23100](#)

phplist.com : News : new stable version 2.10.19

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM](#) [www.phplist.com/?lid=579](#)

NEOHAPSIS - Peace of Mind Through Integrity and Insight

[Exploit](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[BUGTRAQ](#) [20120808 Multiple Vulnerabilities in phpList](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#) [XF nhnlist-delete-sql-injection\(77527\)](#)

No Description Provided

Exploit

OSVDB 84483

osvdb.org

Inactive Link

Not Archived

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	Phplist	Phplist	2.10.1	All	All	All
Application	Phplist	Phplist	2.10.10	All	All	All
Application	Phplist	Phplist	2.10.11	All	All	All
Application	Phplist	Phplist	2.10.12	All	All	All
Application	Phplist	Phplist	2.10.13	All	All	All
Application	Phplist	Phplist	2.10.14	All	All	All
Application	Phplist	Phplist	2.10.15	All	All	All
Application	Phplist	Phplist	2.10.16	All	All	All
Application	Phplist	Phplist	2.10.17	All	All	All
Application	Phplist	Phplist	2.10.2	All	All	All
Application	Phplist	Phplist	2.10.3	All	All	All
Application	Phplist	Phplist	2.10.4	All	All	All
Application	Phplist	Phplist	2.10.5	All	All	All
Application	Phplist	Phplist	2.10.7	All	All	All
Application	Phplist	Phplist	2.10.8	All	All	All
Application	Phplist	Phplist	2.10.9	All	All	All
Application	Phplist	Phplist	2.6.5	All	All	All
Application	Phplist	Phplist	2.7.1	All	All	All
Application	Phplist	Phplist	2.7.2	All	All	All
Application	Phplist	Phplist	2.8.12	All	All	All
Application	Phplist	Phplist	2.8.2	All	All	All
Application	Phplist	Phplist	2.8.7	All	All	All
Application	Phplist	Phplist	2.10.1	All	All	All
Application	Phplist	Phplist	2.10.10	All	All	All

Application	Phplist	Phplist	2.10.11	All	All	All
Application	Phplist	Phplist	2.10.12	All	All	All
Application	Phplist	Phplist	2.10.13	All	All	All
Application	Phplist	Phplist	2.10.14	All	All	All
Application	Phplist	Phplist	2.10.15	All	All	All
Application	Phplist	Phplist	2.10.16	All	All	All
Application	Phplist	Phplist	2.10.17	All	All	All
Application	Phplist	Phplist	2.10.2	All	All	All
Application	Phplist	Phplist	2.10.3	All	All	All
Application	Phplist	Phplist	2.10.4	All	All	All
Application	Phplist	Phplist	2.10.5	All	All	All
Application	Phplist	Phplist	2.10.7	All	All	All
Application	Phplist	Phplist	2.10.8	All	All	All
Application	Phplist	Phplist	2.10.9	All	All	All
Application	Phplist	Phplist	2.6.5	All	All	All
Application	Phplist	Phplist	2.7.1	All	All	All
Application	Phplist	Phplist	2.7.2	All	All	All
Application	Phplist	Phplist	2.8.12	All	All	All
Application	Phplist	Phplist	2.8.2	All	All	All
Application	Phplist	Phplist	2.8.7	All	All	All
Application	Phplist	Phplist	All	All	All	All
cpe:2.3:a:phplist:phplist:2.10.1:*****:						
cpe:2.3:a:phplist:phplist:2.10.10:*****:						
cpe:2.3:a:phplist:phplist:2.10.11:*****:						
cpe:2.3:a:phplist:phplist:2.10.12:*****:						
cpe:2.3:a:phplist:phplist:2.10.13:*****:						
cpe:2.3:a:phplist:phplist:2.10.14:*****:						
cpe:2.3:a:phplist:phplist:2.10.15:*****:						
cpe:2.3:a:phplist:phplist:2.10.16:*****:						
cpe:2.3:a:phplist:phplist:2.10.17:*****:						
cpe:2.3:a:phplist:phplist:2.10.2:*****:						
cpe:2.3:a:phplist:phplist:2.10.3:*****:						
cpe:2.3:a:phplist:phplist:2.10.4:*****:						

cpe:2.3:a:phplist:phplist:2.10.4:*****:
cpe:2.3:a:phplist:phplist:2.10.5:*****:
cpe:2.3:a:phplist:phplist:2.10.7:*****:
cpe:2.3:a:phplist:phplist:2.10.8:*****:
cpe:2.3:a:phplist:phplist:2.10.9:*****:
cpe:2.3:a:phplist:phplist:2.6.5:*****:
cpe:2.3:a:phplist:phplist:2.7.1:*****:
cpe:2.3:a:phplist:phplist:2.7.2:*****:
cpe:2.3:a:phplist:phplist:2.8.12:*****:
cpe:2.3:a:phplist:phplist:2.8.2:*****:
cpe:2.3:a:phplist:phplist:2.8.7:*****:
cpe:2.3:a:phplist:phplist:2.10.1:*****:
cpe:2.3:a:phplist:phplist:2.10.10:*****:
cpe:2.3:a:phplist:phplist:2.10.11:*****:
cpe:2.3:a:phplist:phplist:2.10.12:*****:
cpe:2.3:a:phplist:phplist:2.10.13:*****:
cpe:2.3:a:phplist:phplist:2.10.14:*****:
cpe:2.3:a:phplist:phplist:2.10.15:*****:
cpe:2.3:a:phplist:phplist:2.10.16:*****:
cpe:2.3:a:phplist:phplist:2.10.17:*****:
cpe:2.3:a:phplist:phplist:2.10.2:*****:
cpe:2.3:a:phplist:phplist:2.10.3:*****:
cpe:2.3:a:phplist:phplist:2.10.4:*****:
cpe:2.3:a:phplist:phplist:2.10.5:*****:
cpe:2.3:a:phplist:phplist:2.10.7:*****:
cpe:2.3:a:phplist:phplist:2.10.8:*****:
cpe:2.3:a:phplist:phplist:2.10.9:*****:
cpe:2.3:a:phplist:phplist:2.6.5:*****:
cpe:2.3:a:phplist:phplist:2.7.1:*****:

