



CVE-2006-2065

Published on: 04/27/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:08 PM UTC

CVE-2006-2065

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

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

SQL injection vulnerability in save.php in PHPSurveyor 0.995 and earlier allows remote attackers to execute arbitrary SQL commands via the surveyid cookie. NOTE: this issue could be leveraged to execute arbitrary PHP code, as demonstrated by inserting directory traversal sequences into the database, which are then processed by the `thissurvey['language']` variable.

CVE-2006-2065 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF phpsurveyor-surveyid-shell-execution(25970)
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060420 PHPSurveyor <= 0.995 'save.php/surveyid' remote cmmnds xctn
Secunia - Advisories - PHPSurveyor "surveyid" SQL Injection Vulnerability	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19761
Error 404 :(	Exploit retrogod.altervista.org text/plain	MISC retrogod.altervista.org/phpsurveyor_0995_xpl.html

[cve.report](#)
[Inactive Link](#) [Not Archived](#)

PHPSurveyor SurveyID Parameter SQL Injection Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[🌐 BID 17633](#)

[No Description Provided](#)

[www.osvdb.org](#)

[🌐 OSVDB 24787](#)

[Inactive Link](#) [Not Archived](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[🌐 VUPEN ADV-2006-1451](#)

SecurityTracker.com Archives - PHPSurveyor Input Validation Hole Permits SQL Injection and Lets Remote Users Include and Execute Arbitrary Code

[securitytracker.com](#)
[text/html](#)

[🌐 SPECTRACK 1015970](#)

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	Phpsurveyor	Phpsurveyor	0.96_beta	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.97_beta	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.98_beta	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.98_stable	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.99	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.991	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.992	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.993	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.995	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.96_beta	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.97_beta	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.98_beta	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.98_stable	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.99	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.991	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.992	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.993	All	All	All
Application	Phpsurveyor	Phpsurveyor	0.995	All	All	All

cpe:2.3:a:phpsurveyor:phpsurveyor:0.96_beta:*****:

cpe:2.3:a:phpsurveyor:phpsurveyor:0.97_beta:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.98_beta:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.98_stable:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.99:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.991:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.992:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.993:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.995:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.96_beta:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.97_beta:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.98_beta:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.98_stable:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.99:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.991:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.992:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.993:~::~::~::~:
cpe:2.3:a:phpsurveyor:phpsurveyor:0.995:~::~::~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)