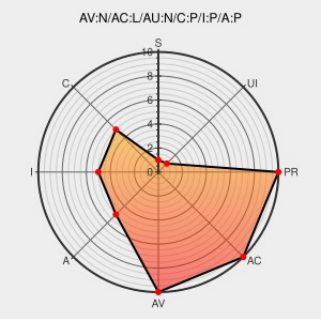
CVE-2004-1785

Published on: 01/03/2004 05:00:00 AM UTC

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

CVE-2004-1785

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



Certain versions of Invision Board from Invision Power Services contain the following vulnerability:

SQL injection vulnerability in calendar.php for Invision Power Board 1.3 allows remote attackers to execute arbitrary SQL commands via the m parameter, which sets the $this->chosen_month variable.

CVE-2004-1785 has been assigned by 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
Secunia - Advisories - Invision Power Board "calendar.php" SQL Injection Vulnerability	Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 10530
Invision Power Board Calendar.PHP SQL Injection Vulnerability	Patch, Vendor Advisory, cve.report (archive), text/html	BID 9353
SecurityFocus	Exploit, Vendor Advisory, www.securityfocus.com, text/html	BUGTRAQ 20040103 [SCSA-025] Invision Power Board SQL Injection Vulnerability
Invision Power Board Input Validation Flaw in 'calendar.php' Permits SQL Injection - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1008589

No Description Provided	Patch Vendor Advisory www.osvdb.org Inactive Link Not Archived	OSVDB 3319
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CONFIRM forums.invisionpower.com/index.php?act=ST&f=1&t=108786

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	Invision Power Services	Invision Board	1.0	All	All	All
Application	Invision Power Services	Invision Board	1.0.1	All	All	All
Application	Invision Power Services	Invision Board	1.1.1	All	All	All
Application	Invision Power Services	Invision Board	1.1.2	All	All	All
Application	Invision Power Services	Invision Board	1.2	All	All	All
Application	Invision Power Services	Invision Board	1.3	All	All	All
Application	Invision Power Services	Invision Board	1.0	All	All	All
Application	Invision Power Services	Invision Board	1.0.1	All	All	All
Application	Invision Power Services	Invision Board	1.1.1	All	All	All
Application	Invision Power Services	Invision Board	1.1.2	All	All	All
Application	Invision Power Services	Invision Board	1.2	All	All	All
Application	Invision Power Services	Invision Board	1.3	All	All	All

cpe:2.3:a:invision_power_services:invision_board:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:invision_power_services:invision_board:1.3:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→