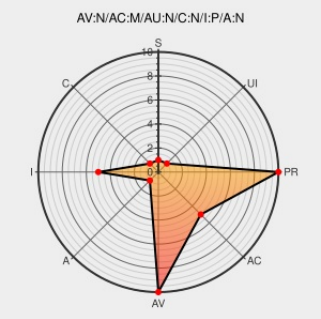
CVE-2004-2735

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:14 PM UTC

CVE-2004-2735

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



Certain versions of P4db from Fredric Fredricson contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in P4DB 2.01 and earlier allows remote attackers to inject arbitrary web script or HTML via (1) SET_PREFERENCES parameter in SetPreferences.cgi; (2) BRANCH parameter in branchView.cgi; (3) FSPC and (4) COMPLETE parameters in changeByUsers.cgi; (5) FSPC, (6) LABEL, (7) EXLABEL, (8) STATUS, (9) MAXCH, (10) FIRSTCH, (11) CHOFFSETDISP, (12) SEARCHDESC, (13) SEARCH_INVERT, (14) USER, (15) GROUP, and (16) CLIENT parameters in changeList.cgi; (17) CH parameter in changeView.cgi; (18) USER parameter in clientList.cgi; (19) CLIENT parameter in clientView.cgi; (20) FSPC parameter in depotTreeBrowser.cgi; (21) FSPC parameter in depotStats.cgi; (22) FSPC, (23) REV, (24) ACT, (25) FSPC2, (26) REV2, (27) CH, and (28) CONTEXT parameters in fileDiffView.cgi; (29) FSPC and (30) REV parameters in fileDownLoad.cgi; (31) FSPC, (32) LISTLAB, and (33) SHOWBRANCH parameters in fileLogView.cgi; (34) FSPC and (35) LABEL parameters in fileSearch.cgi; (36) FSPC, (37) REV, and (38) FORCE parameters in fileViewer.cgi; (39) FSPC parameter in filesChangedSince.cgi; (40) GROUP parameter in groupView.cgi; (41) TYPE, (42) FSPC, and (43) REV parameters in htmlFileView.cgi; (44) CMD parameter in javaDataView.cgi; (45) JOBVIEW and (46) FLD parameters in jobList.cgi; (47) JOB parameter in jobView.cgi; (48) LABEL1 and (49) LABEL2 parameters in labelDiffView.cgi; (50) LABEL parameter in labelView.cgi; (51) FSPC parameter in searchPattern.cgi; (52) TYPE, (53) FSPC, and (54) REV parameters in specialFileView.cgi; (55) GROUPSONLY parameter in userList.cgi; or (56) USER parameter in userView.cgi.

CVE-2004-2735 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Neohapsis Archives - Bugtraq - #0046 - Multiple vulnerabilities in P4DB	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20040505 Multiple vulnerabilities in P4DB
Secunia - Advisories - P4DB Input Validation Vulnerabilities	Vendor Advisory web.archive.org text/html	SECUNIA 11559
P4DB Multiple Input Validation Vulnerabilities	cve.report (archive) text/html	BID 10286
	Patch www.weak.org text/x-diff Inactive Link Not Archived	MISC www.weak.org/~jammer/p4db_v2.01_patch_4.txt
P4DB Input Validation Holes Let Remote Users Execute Arbitrary Shell Commands - SecurityTracker	securitytracker.com text/html	SECTRACK 1010078
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF p4db-url-xss(16070)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 5901

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	Fredric Fredricson	P4db	All	All	All	All

cpe:2.3:a:fredric_fredricson:p4db:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report