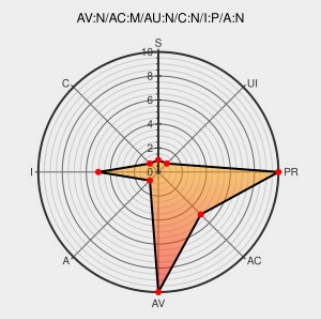
CVE-2004-1797

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

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1797

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



Certain versions of Freznoshop from Freznoshop contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in search.php for FreznoShop 1.3.0 RC1 and earlier allows remote attackers to inject arbitrary web script or HTML via the search parameter.

CVE-2004-1797 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF freznoshop-searchphp-xss(14147)
FreznoShop Input Validation Flaw in 'search' Variable Permits Cross-Site Scripting Attacks - SecurityTracker	Exploit Patch securitytracker.com text/html	SECTRACK 1008606
Secunia - Advisories - FreznoShop "search.php" Cross-Site Scripting Vulnerability	Exploit Patch web.archive.org text/html	SECUNIA 10547
FreznoShop Changelog	web.archive.org text/xml Inactive Link Not Archived	CONFIRM www.freznoshop.com/changelog_en.htm

No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 3335
FreznoShop Search Script Cross-Site Scripting Vulnerability	Exploit cve.report (archive) text/html	BID 9359

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Freznoshop	Freznoshop	1.0	All	All	All
Application	Freznoshop	Freznoshop	1.1.0	All	All	All
Application	Freznoshop	Freznoshop	1.2	All	All	All
Application	Freznoshop	Freznoshop	1.2.1	All	All	All
Application	Freznoshop	Freznoshop	1.2.2	All	All	All
Application	Freznoshop	Freznoshop	1.2.3	All	All	All
Application	Freznoshop	Freznoshop	1.3.0_rc1	All	All	All
Application	Freznoshop	Freznoshop	1.0	All	All	All
Application	Freznoshop	Freznoshop	1.1.0	All	All	All
Application	Freznoshop	Freznoshop	1.2	All	All	All
Application	Freznoshop	Freznoshop	1.2.1	All	All	All
Application	Freznoshop	Freznoshop	1.2.2	All	All	All
Application	Freznoshop	Freznoshop	1.2.3	All	All	All
Application	Freznoshop	Freznoshop	1.3.0_rc1	All	All	All

cpe:2.3:a:freznoshop:freznoshop:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.3.0_rc1:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:freznoshop:freznoshop:1.3.0_rc1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→