



CVE-2004-2603

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

Last Modified on: 03/23/2021 11:28:13 PM UTC

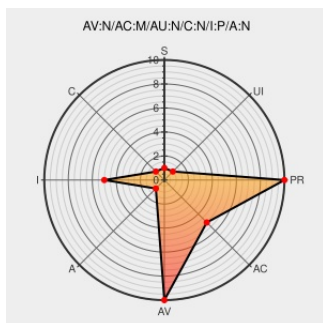
CVE-2004-2603

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Help Center Live](#) from [Ubertec](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the Search module in UberTec Help Center Live (HCL) allows remote attackers to inject arbitrary web script or HTML via the find parameter to index.php.

CVE-2004-2603 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

No Description Provided

Exploit

[www.osvdb.org](#)

[OSVDB 12597](#)

Inactive Link **Not Archived**

Secunia - Advisories - Help Center Live Multiple Vulnerabilities

Vendor Advisory

[web.archive.org](#)

[text/html](#)

[SECUNIA 13652](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

[text/html](#)

[XF help-center-index-xss\(18696\)](#)

Help Center Live Multiple Remote Vulnerabilities

Exploit

[cve.report \(archive\)](#)

[text/html](#)

[BID 12105](#)

Contact Support

[www.gulftech.org](#)

[MISC www.gulftech.org/?](#)

SecurityTracker.com Archives - Help Center Live Include File Flaw Lets Remote Users Execute Arbitrary Commands

Exploit

securitytracker.com

text/html

SECTrack 1012685

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	Ubertec	Help Center Live	1.0	All	All	All
Application	Ubertec	Help Center Live	1.2	All	All	All
Application	Ubertec	Help Center Live	1.2.1	All	All	All
Application	Ubertec	Help Center Live	1.2.2	All	All	All
Application	Ubertec	Help Center Live	1.2.3	All	All	All
Application	Ubertec	Help Center Live	1.2.4	All	All	All
Application	Ubertec	Help Center Live	1.2.5	All	All	All
Application	Ubertec	Help Center Live	1.2.6	All	All	All
Application	Ubertec	Help Center Live	1.0	All	All	All
Application	Ubertec	Help Center Live	1.2	All	All	All
Application	Ubertec	Help Center Live	1.2.1	All	All	All
Application	Ubertec	Help Center Live	1.2.2	All	All	All
Application	Ubertec	Help Center Live	1.2.3	All	All	All
Application	Ubertec	Help Center Live	1.2.4	All	All	All
Application	Ubertec	Help Center Live	1.2.5	All	All	All
Application	Ubertec	Help Center Live	1.2.6	All	All	All

cpe:2.3:a:ubertec:help_center_live:1.0:*:*:*:*:*:

cpe:2.3:a:ubertec:help_center_live:1.2:*:*:*:*:*:

cpe:2.3:a:ubertec:help_center_live:1.2.1:*:*:*:*:*:

cpe:2.3:a:ubertec:help_center_live:1.2.2:*:*:*:*:*:

cpe:2.3:a:ubertec:help_center_live:1.2.3:*:*:*:*:*:

cpe:2.3:a:ubertec:help_center_live:1.2.4:*:*:*:*:*:

cpe:2.3:a:ubertec:help_center_live:1.2.5:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2.6:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.0:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2.1:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2.2:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2.3:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2.4:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2.5:*:*:*:*:*:
cpe:2.3:a:ubertec:help_center_live:1.2.6:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)