



CVE-2006-2023

Published on: 04/25/2006 12:00:00 AM UTC

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

CVE-2006-2023

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Fenice](#) from [Ls3](#) contain the following vulnerability:

Integer overflow in the RTSP_msg_len function in rtsp/RTSP_msg_len.c in Fenice 1.10 and earlier allows remote attackers to cause a denial of service (application crash) via a large HTTP Content-Length value, which leads to an invalid memory access.

CVE-2006-2023 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

SecurityReason - Buffer-overflow and crash in Fenice OMS 1.10

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

[SREASON 794](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 24882](#)

Inactive Link Not Archived

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-1491](#)

Fenice Remote Buffer Overflow and Denial Of Service Vulnerabilities

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

[BID 17678](#)

SecurityFocus

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

[BUGTRAQ 20060607 Re: Buffer-overflow and crash in Fenice OMS 1.10](#)

SecurityFocus

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

BUGTRAQ 20060423 Buffer-overflow and crash in Fenice OMS 1.10

[aluigi.altervista.org](#)
[text/x-c](#)

MISC aluigi.altervista.org/adv/fenicex-adv.txt

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

XF fenice-contentlength-dos(26080)

Fenice HTTP Request Handling Two Vulnerabilities - Advisories - Secunia

[Exploit](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

SECUNIA 19770

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	Ls3	Fenice	All	All	All	All

cpe:2.3:a:ls3:fenice:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →