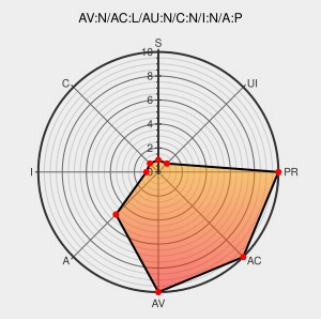
CVE-2006-2023

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 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 Inactive Link Not Archived	OSVDB 24882
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

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→