CVE-2008-4771

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-4771
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-28 19:20:00 UTC
Updated	2017-09-29 01:32:00 UTC
Description	Stack-based buffer overflow in VATDecoder.VatCtrl.1 ActiveX control in (1) 4xem VatCtrl Class (VATDecoder.dll 1.0.0.27 a

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	4xem	Vatctrl Class	1.0.0.27	All	All	All
Application	4xem	Vatctrl Class	1.0.0.51	All	All	All
Application	4xem	Vatctrl Class	1.0.0.27	All	All	All
Application	4xem	Vatctrl Class	1.0.0.51	All	All	All
Application	D-link	Mpeg4 Shm Audio Control	1.7.0.5	All	All	All
Application	D-link	Mpeg4 Shm Audio Control	1.7.0.5	All	All	All
Application	Vivotek	Rtsp Mpeg4 Sp Control	2.0.0.39	All	All	All
Application	Vivotek	Rtsp Mpeg4 Sp Control	2.0.0.39	All	All	All

References

Reference	So
D-Link MPEG4 SHM (Audio) Control ActiveX Control "Url" Property Buffer Overflow - Advisories - Secunia	SE
RTSP MPEG4 SP Control ActiveX Control "Url" Property Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SE
42378	OS
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VU
IBM X-Force Exchange	XF
Various IP Security Camera ActiveX Controls 'url' Attribute Buffer Overflow Vulnerability	BID

D-Link MPEG4 SHM Audio Control (VAPGDecoder.dll 1.7.0.5) remote overflow - SecurityReason.com	SR
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VU
43007	OS
4XEM VatDecoder VatCtrl Class ActiveX Control "Url" Property Buffer Overflow - Advisories - Secunia	SE
IBM X-Force Exchange	XF
IBM X-Force Exchange	XF
D-Link MPEG4 SHM Audio Control (VAPGDecoder.dll 1.7.0.5) BOF Exploit	EX
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VU
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.