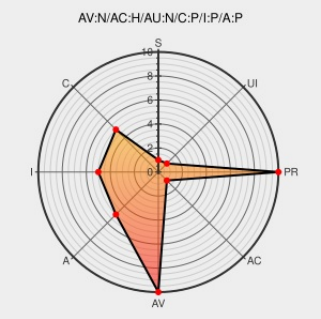
CVE-2006-1385

Published on: 03/24/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-1385

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



Certain versions of Kismac from Kismac contain the following vulnerability:

Stack-based buffer overflow in the parseTaggedData function in WavePacket.mm in KisMAC R54 through R73p allows remote attackers to execute arbitrary code via multiple SSIDs in a Cisco vendor tag in a 802.11 management frame.

CVE-2006-1385 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityReason	securityreason.com text/html	SREASON 609
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24072
[Full-disclosure] Advisory 03/2006: KisMAC Cisco Vendor Tag Encapsulated SSID Overflow	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20060323 Advisory 03/2006: KisMAC Cisco Vendor Tag Encapsulated SSID Overflow
Secunia - Advisories - KisMAC Cisco Vendor Tag SSID Parsing Buffer Overflow	Vendor Advisory web.archive.org text/html	SECUNIA 19354
KisMAC Cisco Vendor Tag Remote Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 17198

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF kismac-80211-parsing-bo(25422)
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060323 Advisory 03/2006: KisMAC Cisco Vendor Tag Encapsulated SSID Overflow
Hardened-PHP Project - PHP Security - Advisory 03/2006	www.hardened-php.net text/html	MISC www.hardened-php.net/advisory_032006.115.html
Webmail- OVH	www.vupen.com text/html	VUPEN ADV-2006-1070
[113] - KisMAC - Trac	kismac.de text/html	CONFIRM kismac.de/_trac/changeset/113

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kismac	Kismac	0.10a	All	All	All
Application	Kismac	Kismac	0.11a	All	All	All
Application	Kismac	Kismac	0.12a	All	All	All
Application	Kismac	Kismac	0.1a	All	All	All
Application	Kismac	Kismac	0.1b	All	All	All
Application	Kismac	Kismac	0.1c	All	All	All
Application	Kismac	Kismac	0.2a	All	All	All
Application	Kismac	Kismac	0.5d	All	All	All
Application	Kismac	Kismac	0.5d4	All	All	All
Application	Kismac	Kismac	0.10a	All	All	All
Application	Kismac	Kismac	0.11a	All	All	All
Application	Kismac	Kismac	0.12a	All	All	All
Application	Kismac	Kismac	0.1a	All	All	All
Application	Kismac	Kismac	0.1b	All	All	All
Application	Kismac	Kismac	0.1c	All	All	All
Application	Kismac	Kismac	0.2a	All	All	All
Application	Kismac	Kismac	0.5d	All	All	All
Application	Kismac	Kismac	0.5d4	All	All	All

cpe:2.3:a:kismac:kismac:0.10a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.11a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.12a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.1a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.1b:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.1c:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.2a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.5d:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.5d4:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.10a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.11a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.12a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.1a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.1b:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.1c:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.2a:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.5d:*:*:*:*:*:*:*

cpe:2.3:a:kismac:kismac:0.5d4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→