



CVE-2005-2627

Published on: 08/19/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2627

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

Multiple integer underflows in Kismet before 2005-08-R1 allow remote attackers to execute arbitrary code via (1) kernel headers in a pcap file or (2) data frame dissection, which leads to heap-based buffer overflows.

CVE-2005-2627 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Security Announcement

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[ot](#) [SUSE SUSE-SR:2005:020](#)

Secunia - Advisories - Kismet Multiple Vulnerabilities

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[X](#) [SECUNIA 16447](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)

[text/html](#)

[VUPEN ADV-2005-1422](#)

Kismet Multiple Remote Vulnerabilities

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

[text/html](#)

[BID 14430](#)

Kismet

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[CONFIRM](#) [www.kismetwireless.net/blog/?entry=/kismet/entry-1124158146.txt](#)

404 Not Found	www.kismetwireless.net text/plain Inactive Link Not Archived	 CONFIRM www.kismetwireless.net/CHANGELOG
Secunia - Advisories - Debian update for kismet	web.archive.org text/html	 SECUNIA 16634
Debian -- Security Information -- DSA-788-1 kismet	www.debian.org Deprecated Link text/html	 DEBIAN DSA-788
Gentoo update for Kismet - Secunia.com	web.archive.org text/html	 SECUNIA 16477
Gentoo Linux Documentation -- Kismet: Multiple vulnerabilities	www.gentoo.org text/html	 GENTOO GLSA-200508-10
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	Kismet	Kismet	2.4.5	All	All	All
Application	Kismet	Kismet	2.4.6	All	All	All
Application	Kismet	Kismet	2.6.0	All	All	All
Application	Kismet	Kismet	2.8.0	All	All	All
Application	Kismet	Kismet	2.8.0a	All	All	All
Application	Kismet	Kismet	2.8.1	All	All	All
Application	Kismet	Kismet	2004-02_r1	All	All	All
Application	Kismet	Kismet	2004-04_r1	All	All	All
Application	Kismet	Kismet	2004-04_r1a	All	All	All
Application	Kismet	Kismet	2004-10_r1	All	All	All
Application	Kismet	Kismet	2005-01_r1	All	All	All
Application	Kismet	Kismet	2005-04_r1	All	All	All
Application	Kismet	Kismet	2005-06_r1	All	All	All
Application	Kismet	Kismet	2005-07_bsd	All	All	All
Application	Kismet	Kismet	2005-07_r1	All	All	All
Application	Kismet	Kismet	2005-07_r1a	All	All	All
Application	Kismet	Kismet	2.4.5	All	All	All
Application	Kismet	Kismet	2.4.6	All	All	All
Application	Kismet	Kismet	2.4.6	All	All	All

Application	Kismet	Kismet	2.6.0	All	All	All
Application	Kismet	Kismet	2.8.0	All	All	All
Application	Kismet	Kismet	2.8.0a	All	All	All
Application	Kismet	Kismet	2.8.1	All	All	All
Application	Kismet	Kismet	2004-02_r1	All	All	All
Application	Kismet	Kismet	2004-04_r1	All	All	All
Application	Kismet	Kismet	2004-04_r1a	All	All	All
Application	Kismet	Kismet	2004-10_r1	All	All	All
Application	Kismet	Kismet	2005-01_r1	All	All	All
Application	Kismet	Kismet	2005-04_r1	All	All	All
Application	Kismet	Kismet	2005-06_r1	All	All	All
Application	Kismet	Kismet	2005-07_bsd	All	All	All
Application	Kismet	Kismet	2005-07_r1	All	All	All
Application	Kismet	Kismet	2005-07_r1a	All	All	All
cpe:2.3:a:kismet:kismet:2.4.5:*****:						
cpe:2.3:a:kismet:kismet:2.4.6:*****:						
cpe:2.3:a:kismet:kismet:2.6.0:*****:						
cpe:2.3:a:kismet:kismet:2.8.0:*****:						
cpe:2.3:a:kismet:kismet:2.8.0a:*****:						
cpe:2.3:a:kismet:kismet:2.8.1:*****:						
cpe:2.3:a:kismet:kismet:2004-02_r1:*****:						
cpe:2.3:a:kismet:kismet:2004-04_r1:*****:						
cpe:2.3:a:kismet:kismet:2004-04_r1a:*****:						
cpe:2.3:a:kismet:kismet:2004-10_r1:*****:						
cpe:2.3:a:kismet:kismet:2005-01_r1:*****:						
cpe:2.3:a:kismet:kismet:2005-04_r1:*****:						
cpe:2.3:a:kismet:kismet:2005-06_r1:*****:						
cpe:2.3:a:kismet:kismet:2005-07_bsd:*****:						
cpe:2.3:a:kismet:kismet:2005-07_r1:*****:						
cpe:2.3:a:kismet:kismet:2005-07_r1a:*****:						
cpe:2.3:a:kismet:kismet:2.4.5:*****:						
cpe:2.3:a:kismet:kismet:2.4.6:*****:						

cpe:2.3:a:kismet:kismet:2.4.b:*****:
cpe:2.3:a:kismet:kismet:2.6.0:*****:
cpe:2.3:a:kismet:kismet:2.8.0:*****:
cpe:2.3:a:kismet:kismet:2.8.0a:*****:
cpe:2.3:a:kismet:kismet:2.8.1:*****:
cpe:2.3:a:kismet:kismet:2004-02_r1:*****:
cpe:2.3:a:kismet:kismet:2004-04_r1:*****:
cpe:2.3:a:kismet:kismet:2004-04_r1a:*****:
cpe:2.3:a:kismet:kismet:2004-10_r1:*****:
cpe:2.3:a:kismet:kismet:2005-01_r1:*****:
cpe:2.3:a:kismet:kismet:2005-04_r1:*****:
cpe:2.3:a:kismet:kismet:2005-06_r1:*****:
cpe:2.3:a:kismet:kismet:2005-07_bsd:*****:
cpe:2.3:a:kismet:kismet:2005-07_r1:*****:
cpe:2.3:a:kismet:kismet:2005-07_r1a:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)