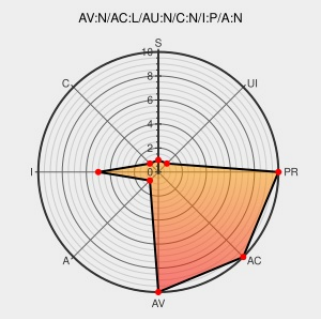
CVE-2005-2359

Published on: 08/01/2005 12:00:00 AM UTC

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

CVE-2005-2359

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



Certain versions of Freebsd from Freebsd contain the following vulnerability:

The AES-XCBC-MAC algorithm in IPsec in FreeBSD 5.3 and 5.4, when used for authentication without other encryption, uses a constant key instead of the one that was assigned by the system administrator, which can allow remote attackers to spoof packets to establish an IPsec session.

CVE-2005-2359 has been assigned by secteam@freebsd.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
SecurityTracker.com Archives - FreeBSD Bug in IPSec AES-XCBC-MAC Algorithm May Cause the Incorrect Key to Be Used	securitytracker.com text/html	SECTRACK 1014586
	ftp.freebsd.org text/plain Inactive Link Not Archived	FREEBSD FreeBSD-SA-05:19
BSD IPsec Session AES-XCBC-MAC Authentication Constant Key Usage Vulnerability	cve.report (archive) text/html	BID 14394
Secunia - Advisories - FreeBSD IPsec AES-XCBC-MAC Authentication Security Issue	Patch Vendor Advisory web.archive.org text/html	SECUNIA 16244

IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF freebsd-aesxcbcmac-security-bypass(21551)

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
Operating System	Freebsd	Freebsd	5.3	All	All	All
Operating System	Freebsd	Freebsd	5.4	All	All	All
Operating System	Freebsd	Freebsd	5.3	All	All	All
Operating System	Freebsd	Freebsd	5.4	All	All	All

cpe:2.3:o:freebsd:freebsd:5.3:*:*:*:*:*:*:*

cpe:2.3:o:freebsd:freebsd:5.4:*:*:*:*:*:*:*

cpe:2.3:o:freebsd:freebsd:5.3:*:*:*:*:*:*:*

cpe:2.3:o:freebsd:freebsd:5.4:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report