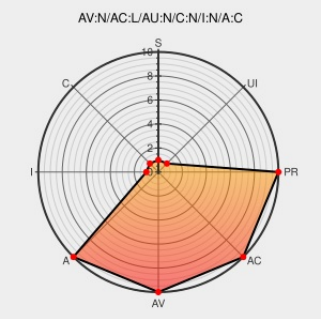
CVE-2005-4570

Published on: 12/29/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-4570

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



Certain versions of Forticlient from Fortinet contain the following vulnerability:

The Internet Key Exchange version 1 (IKEv1) implementations in Fortinet FortiOS 2.50, 2.80 and 3.0, FortiClient 2.0,; and FortiManager 2.80 and 3.0 allow remote attackers to cause a denial of service (termination of a process that is automatically restarted) via IKE packets with invalid values of certain IPSec attributes, as demonstrated by the PROTOS ISAKMP Test Suite for IKEv1. NOTE: due to the lack of details in the vendor advisory, it is unclear which of CVE-2005-3666, CVE-2005-3667, and/or CVE-2005-3668 this issue applies to.

CVE-2005-4570 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
FortiGuard Center - Advisory - IKE ISAKMP (VU#226364) vulnerabilities	Patch, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www.fortinet.com/FortiGuardCenter/VU226364.html
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com, text/html	VUPEN ADV-2006-0182
Secunia - Advisories - Fortinet Products ISAKMP IKE Message Processing Vulnerabilities	web.archive.org	SECUNIA 18446

Message Processing Vulnerabilities	text/html	
Multiple Fortinet Products IKE Exchange Denial Of Service Vulnerabilities	cve.report (archive) text/html	BID 15997

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
Hardware	Fortinet	Forticlient	2.0	All	All	All
Hardware	Fortinet	Forticlient	2.0	All	All	All
Hardware	Fortinet	Fortimanager	2.80	All	All	All
Hardware	Fortinet	Fortimanager	3.0	All	All	All
Hardware	Fortinet	Fortimanager	2.80	All	All	All
Hardware	Fortinet	Fortimanager	3.0	All	All	All
Operating System	Fortinet	Fortios	2.50	All	All	All
Operating System	Fortinet	Fortios	2.80	All	All	All
Operating System	Fortinet	Fortios	3.0	All	All	All
Operating System	Fortinet	Fortios	2.50	All	All	All
Operating System	Fortinet	Fortios	2.80	All	All	All
Operating System	Fortinet	Fortios	3.0	All	All	All

cpe:2.3:h:fortinet:forticlient:2.0:*:*:*:*:*:*:*:

cpe:2.3:h:fortinet:forticlient:2.0:*:*:*:*:*:*:*:

cpe:2.3:h:fortinet:fortimanager:2.80:*:*:*:*:*:*:*:

cpe:2.3:h:fortinet:fortimanager:3.0:*:*:*:*:*:*:*:

cpe:2.3:h:fortinet:fortimanager:2.80:*:*:*:*:*:*:*:

cpe:2.3:h:fortinet:fortimanager:3.0:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:2.50:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:2.80:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:3.0:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:2.50:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:2.80:*:*:*:*:*:*:*:

cpe:2.3:o:fortinet:fortios:3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→