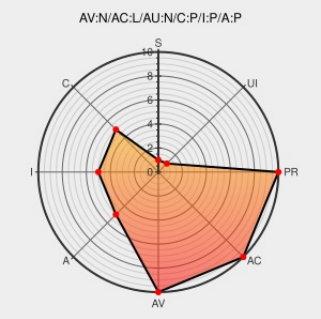
CVE-2005-4437

Published on: 12/20/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:20 PM UTC

CVE-2005-4437

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



Certain versions of Extended Interior Gateway Routing Protocol from Extended Interior Gateway Routing Protocol contain the following vulnerability:

MD5 Neighbor Authentication in Extended Interior Gateway Routing Protocol (EIGRP) 1.2, as implemented in Cisco IOS 11.3 and later, does not include the Message Authentication Code (MAC) in the checksum, which allows remote attackers to sniff message hashes and (1) replay EIGRP HELLO messages or (2) cause a denial of service by sending a large number of spoofed EIGRP neighbor announcements, which results in an ARP storm on the local network.

CVE-2005-4437 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2005-3008
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051219 Authenticated EIGRP DoS / Information leak
Authenticated EIGRP DoS / Information leak - SecurityReason.com	securityreason.com text/html	SREASON 274
[Full-disclosure] Authenticated EIGRP DoS / Information leak	Vendor Advisory	FULLDISC 20051219

[Full-disclosure] Authenticated EIGRP DoS / Information leak	web.archive.org text/html Inactive Link Not Archived	FULLDISC 20051220 Authenticated EIGRP DoS / Information leak
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20051220 Re: Unauthenticated EIGRP DoS
SecurityTracker.com Archives - Cisco IOS EIGRP Bugs Let Remote Users Deny Service or Obtain Potentially Sensitive Information	securitytracker.com text/html	SECTRACK 1015382
Cisco EIGRP Protocol HELLO Packet Replay Vulnerability	cve.report (archive) text/html	BID 15970
'[Full-disclosure] RE: Authenticated EIGRP DoS / Information leak' - MARC	marc.info text/html	FULLDISC 20051220 RE: Authenticated EIGRP DoS / Information leak
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:5741

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	Extended Interior Gateway Routing Protocol	Extended Interior Gateway Routing Protocol	1.2	All	All	All
Application	Extended Interior Gateway Routing Protocol	Extended Interior Gateway Routing Protocol	1.2	All	All	All

cpe:2.3:a:extended_interior_gateway_routing_protocol:extended_interior_gateway_routing_protocol:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:extended_interior_gateway_routing_protocol:extended_interior_gateway_routing_protocol:1.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→