



CVE-2017-6444

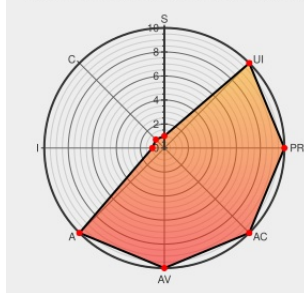
Published on: 03/11/2017 12:00:00 AM UTC

Last Modified on: 05/25/2021 03:03:00 PM UTC

CVE-2017-6444

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H



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

The MikroTik Router hAP Lite 6.25 has no protection mechanism for unsolicited TCP ACK packets in the case of a fast network connection, which allows remote attackers to cause a denial of service (CPU consumption) by sending many ACK packets. After the attacker stops the exploit, the CPU usage is 100% and the router requires a reboot for

normal operation.

CVE-2017-6444 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

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
MikroTik Router Denial Of Service ARP Table OverFlow - CXSecurity.com	Exploit Third Party Advisory	CX MISC cxsecurity.com/issue/WLB-2017030029

cxsecurity.com
text/html

Mikrotik Hap Lite 6.25 Denial Of Service ≈ Packet Storm

Exploit
Third Party Advisory
VDB Entry
packetstormsecurity.com
text/html

MISC packetstormsecurity.com/files/141449/Mikrotik-Hap-Lite-6.25-Denial-Of-Service.html

Exploit – Page 41601 – Exploits Database

www.exploit-db.com
Proof of Concept
text/html

EXPLOIT-DB 41601

MikroTik Router Denial Of Service | ARP Table OverFlow - Exploitalert

Exploit
Third Party Advisory
www.exploitalert.com
text/html

MISC www.exploitalert.com/view-details.html?id=26137

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	Mikrotik	Routeros	6.25	All	All	All
Hardware 	Mikrotik	Router Hap Lite	-	All	All	All
Hardware 	Mikrotik	Router Hap Lite	-	All	All	All
Operating System	Mikrotik	Router Hap Lite Firmware	6.25	All	All	All
Operating System	Mikrotik	Router Hap Lite Firmware	6.25	All	All	All
cpe:2.3:o:mikrotik:routeros:6.25:~::~~::~~::						
cpe:2.3:h:mikrotik:router_hap_lite:~::~~::~~::						
cpe:2.3:h:mikrotik:router_hap_lite:~::~~::~~::						
cpe:2.3:o:mikrotik:router_hap_lite_firmware:6.25:~::~~::~~::						
cpe:2.3:o:mikrotik:router_hap_lite_firmware:6.25:~::~~::~~::						

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](#)