

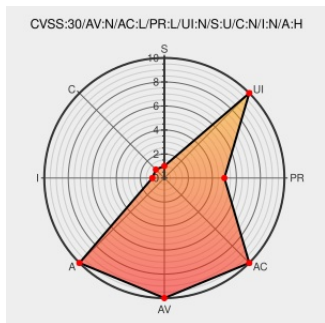


# CVE-2019-13954

Published on: 07/26/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:46 PM UTC

## CVE-2019-13954

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

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

Mikrotik RouterOS before 6.44.5 (long-term release tree) is vulnerable to memory exhaustion. By sending a crafted HTTP request, an authenticated remote attacker can crash the HTTP server and in some circumstances reboot the system. Malicious code cannot be injected.

CVE-2019-13954 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>LOW</b>          | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>SINGLE</b>       |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>NONE</b>            | <b>NONE</b>       | <b>COMPLETE</b>     |

## CVE References

| Description                                                       | Tags                                                                                                                              | Link                                                                                             |
|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Full Disclosure: Two vulnerabilities found in MikroTik's RouterOS | <a href="#">Mailing List</a><br><a href="#">Third Party Advisory</a><br><a href="#">seclists.org</a><br><a href="#">text/html</a> | <a href="https://seclists.org/misc/2019/Jul/20">MISC seclists.org/fulldisclosure/2019/Jul/20</a> |

There are currently no QIDs associated with this CVE

| Type                                              | Vendor   | Product  | Version | Update | Edition | Language |
|---------------------------------------------------|----------|----------|---------|--------|---------|----------|
| Operating System                                  | Mikrotik | Routeros | All     | All    | All     | All      |
| Operating System                                  | Mikrotik | Routeros | 6.45    | All    | All     | All      |
| Operating System                                  | Mikrotik | Routeros | All     | All    | All     | All      |
| Operating System                                  | Mikrotik | Routeros | 6.45    | All    | All     | All      |
| cpe:2.3:o:mikrotik:routeros:*.*.*.*.*.*.*.*.      |          |          |         |        |         |          |
| cpe:2.3:o:mikrotik:routeros:6.45:*.*.*.*.*.*.*.*. |          |          |         |        |         |          |
| cpe:2.3:o:mikrotik:routeros:*.*.*.*.*.*.*.*.      |          |          |         |        |         |          |
| cpe:2.3:o:mikrotik:routeros:6.45:*.*.*.*.*.*.*.*. |          |          |         |        |         |          |

Next ID→