



CVE-2018-1156

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-1156
State	PUBLIC
Assigner	vulnreport@tenable.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-23 19:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Mikrotik RouterOS before 6.42.7 and 6.40.9 is vulnerable to stack buffer overflow through the license upgrade interface. Th

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Mikrotik	Routeros	All	All	All	All
Operating System	Mikrotik	Routeros	All	All	All	All
Operating System	Mikrotik	Routeros	All	All	All	All
Operating System	Mikrotik	Routeros	All	All	All	All

References

Reference	Source	Link	Tags
MikroTik Routers and Wireless - Software	CONFIRM	mikrotik.com	Vendor Adv
[R1] Mikrotik RouterOS Multiple Authenticated Vulnerabilities - Research Advisory Tenable®	MISC	www.tenable.com	Exploit, Thir
MikroTik Routers and Wireless - Software	CONFIRM	mikrotik.com	Vendor Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)