

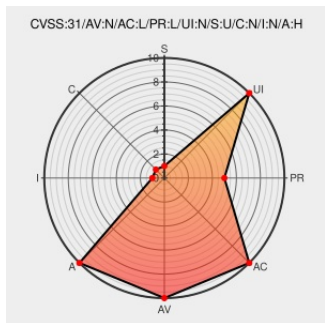


CVE-2020-20220

Published on: 05/18/2021 12:00:00 AM UTC

Last Modified on: 05/21/2021 07:19:00 PM UTC

CVE-2020-20220

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

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

Mikrotik RouterOs prior to stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/bfd process. An authenticated remote attacker can cause a Denial of Service (NULL pointer dereference).

CVE-2020-20220 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
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
MikroTik Routers and Wireless	mikrotik.com text/html	MISC mikrotik.com/
MikroTik RouterOS Memory Corruption ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162533/MikroTik-RouterOS-Memory-Corruption.html

There are currently no QIDs associated with this CVE

PoC for exploiting CVE-2020-20220

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Mikrotik	Routers	All	All	All	All
cpe:2.3:o:mikrotik:routers:*:*:*:*:*:*						

No vendor comments have been submitted for this CVE

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-20220 : Mikrotik RouterOs prior to stable 6.47 suffers from a memory corruption vulnerability in the /nova... twitter.com/i/web/status/1...	2021-05-18 20:04:21
/r/netcve	CVE-2020-20220	2021-05-18 20:41:33

Next ID→