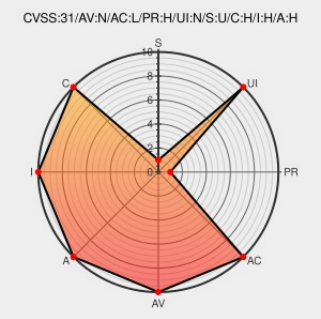
CVE-2020-25206

Published on: 07/20/2021 12:00:00 AM UTC

Last Modified on: 10/05/2022 04:21:00 PM UTC

CVE-2020-25206

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



Certain versions of B5 from Mimosa contain the following vulnerability:

The web console for Mimosa B5, B5c, and C5x firmware through 2.8.0.2 allows authenticated command injection in the Throughput, WANStats, PhyStats, and QosStats API classes. An attacker with access to a web console account may execute operating system commands on affected devices by sending crafted POST requests to the affected endpoints (/core/api/calls/Throughput.php, /core/api/calls/WANStats.php, /core/api/calls/PhyStats.php, /core/api/calls/QosStats.php). This results in the complete takeover of the vulnerable device. This vulnerability does not occur in the older 1.5.x firmware versions.

CVE-2020-25206 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

CWE - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') (4.9)	cwe.mitre.org text/html	MISC cwe.mitre.org/data/definitions/78.html
Advisories	labs.f-secure.com text/html	MISC labs.f-secure.com/advisories/
Mimosa PTP Devices - Multiple Vulnerabilities	labs.f-secure.com text/html	MISC labs.f-secure.com/advisories/mimosa-ptp-devices-multiple-vulnerabilities/

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
Hardware	Mimosa	B5	-	All	All	All
Hardware	Mimosa	B5c	-	All	All	All
Operating System	Mimosa	B5c Firmware	All	All	All	All
Operating System	Mimosa	B5 Firmware	All	All	All	All
Hardware	Mimosa	C5c	-	All	All	All
Operating System	Mimosa	C5c Firmware	All	All	All	All

cpe:2.3:h:mimosa:b5:-:*:*:*:*:*:*:*:

cpe:2.3:h:mimosa:b5c:-:*:*:*:*:*:*:*:

cpe:2.3:o:mimosa:b5c_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:mimosa:b5_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:mimosa:c5c:-:*:*:*:*:*:*:*:

cpe:2.3:o:mimosa:c5c_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-25206 : The web console for Mimosa B5, B5c, and C5x firmware through 2.8.0.2 allows authenticated command… twitter.com/i/web/status/1…	2021-07-20 19:04:11
	New vulnerability on the NVD: CVE-2020-25206 ift.tt/3zIlGwy	2021-07-20

@WesUncensored	New vulnerability on the NVD: CVE-2020-25206 ift.tt/3zll6wy	2021-07-20 20:48:16
@Velletron	CVE-2020-25206 ift.tt/3zll6wy #CVE #Vulnerability	2021-07-20 20:54:05
@xanadulinux	CVE-2020-25206 ift.tt/3zll6wy	2021-07-20 21:02:16
@workentin	New vulnerability on the NVD: CVE-2020-25206 ift.tt/3zll6wy	2021-07-20 21:05:22
@LinInfoSec	Php - CVE-2020-25206: labs.f-secure.com/advisories/	2021-07-30 16:35:07
/r/netcve	CVE-2020-25206	2021-07-20 19:40:33

← Previous ID

Next ID→