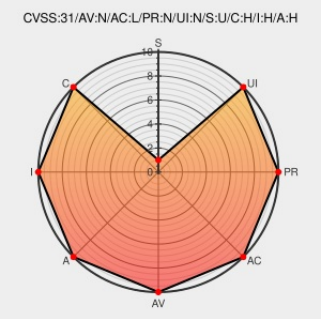
CVE-2020-15920

Published on: 07/23/2020 12:00:00 AM UTC

Last Modified on: 01/20/2023 08:44:00 PM UTC

CVE-2020-15920

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



Certain versions of Eframework from Midasolutions contain the following vulnerability:

There is an OS Command Injection in Mida eFramework through 2.9.0 that allows an attacker to achieve Remote Code Execution (RCE) with administrative (root) privileges. No authentication is required.

CVE-2020-15920 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Mida Solutions eFramework Multiple Vulnerabilities | elbae on github.io	Exploit Third Party Advisory elbae.github.io text/html	MISC elbae.github.io/jekyll/update/2020/07/14/vulns-01.html

Mida eFramework 2.9.0 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/158991/Mida-eFramework-2.9.0-Remote-Code-Execution.html
Mida Solutions eFramework ajaxreq.php Command Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159194/Mida-Solutions-eFramework-ajaxreq.php-Command-Injection.html

There are currently no QIDs associated with this CVE

Exploit/POC from Github

There is an OS Command Injection in Mida eFramework through 2.9.0 that allows an attacker to achieve Remote Code Exec…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Midasolutions	Eframework	All	All	All	All

cpe:2.3:a:midasolutions:eframework:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→