

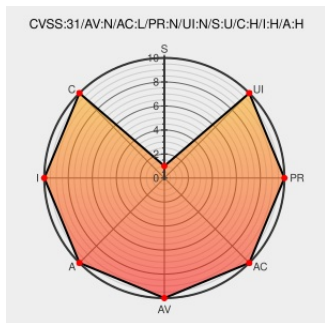


# CVE-2020-15920

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 [M](#) [cve@mitre.org](mailto: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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **10 - HIGH**

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

## CVE References

| Description                                                             | Tags                                                                                                                            | Link                                                                        |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Mida Solutions eFramework Multiple Vulnerabilities   elbae on github.io | <a href="#">Exploit</a><br><a href="#">Third Party Advisory</a><br><a href="#">elbae.github.io</a><br><a href="#">text/html</a> | <a href="#">MISC elbae.github.io/jekyll/update/2020/07/14/vulns-01.html</a> |

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

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](mailto:comment@cve.report).

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→