Mida Solutions eFramework Multiple Vulnerabilities

Jul 14, 2020

Title: Mida Solutions eFramework Multiple Vulnerabilities

Date: 21/05/2020 (Last Update 24/07/2020)

Author: Andrea Baesso

Reference: https://elbae.github.io/jekyll/update/2020/07/14/vulns-01.html

Vendor Homepage: https://www.midasolutions.com/

Software Link: http://ova-efw.midasolutions.com/

Versions: <=2.9.0

Tested on: 2.8.9, 2.9.0

CVE: CVE-2020-15918, CVE-2020-15919, CVE-2020-15920, CVE-2020-15921, CVE-2020-15922, CVE-2020-15923, CVE-2020-15924

Abstract

During my spare time I analized *independently* a publicly available product, not extremely widespread, but still used around the world. I found several vulnerabilities, reported to the vendor which **silently fixed** a few of them without a single answer to my e-mails.

Vendor Description

> *Mida Solutions is a high skilled Italian company focusing on Unified Communication. Since 2004, it offers unique expertise and a complete suite of advanced services and voice applications with the mission to provide value added innovative technologies for communication.*
>
> *–https://www.midasolutions.com/it/*

> *Mida eFramework is a complete suite of video and voice applications, compatible with almost all major UC platforms. The suite includes attendant console, recorder, fax server, billing, queue manager, automated attendant, mobile apps, phone services.*
>
> *–https://www.midasolutions.com/it/portfolio-item/mida-eframework/*

The product comes as a preconfigured Open Virtual Appliance (OVA) which can be downloaded from the company's website and easily imported in production environments.

Business recommendation

The vendor did not respond to my communication attempts, hence no patch is available. A third party patch may be released either if the company will not fix the product in the next months or at request. Do not expose the software on WAN. Use ACL to allow or deny access to the software.

Vulnerability highlight

Several vulnerabilities allow unauthenticated Remote Code Execution (RCE) through Command Injection on the system with administrative privileges. Any attacker may leverage the issue to obtain a remote shell, or directly execute system commands with the output returned in text format, and possibly access the internal network (if exposed in WAN).

Vulnerability Overview/Description:

1. OS Command Injection Remote Code Execution Vulnerability (RCE) and Denial of Service (Dos) (CVE-2020-15920)

(Unauthenticated) There is an OS Command Injection in eFramework <= 2.9.0 that allows an attacker a Remote Code Execution (RCE) with administrative (root) privileges. No authentication is required. The injection point resides on an *undisclosed* PHP page which can be targeted with either GET or POST malicious payload.

- Impact: OS Code Execution
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

2,3,4. OS Command Injection RCE (CVE-2020-15922)

(Unauthenticated <= 2.8.9, Authenticated 2.9.0) There is an OS Command Injection in eFramework <= 2.8.9 that allows an attacker to trigger a Remote Code Execution (RCE), with administrative (root) privileges, through OS Command Injection. No authentication is required. The injection point resides on an *undisclosed* PHP page. Impact: OS Code Execution

- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (<= 2.8.9)
- CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H (2.9.0)

5. SQL Injection (CVE-2020-15924)

(Unauthenticated) There is an SQL Injection in eFramework <= 2.9.0 that leverages to Information Disclosure. No authentication is required. The injection point resides in one of the authentication parameters.

- Impact: Database Exfiltration, Information Disclosure, Privilege Escalation
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

6. Path Traversal (CVE-2020-15923)

(Unauthenticated, with root level access <= 2.8.9, with user level access 2.9.0) eFramework <= 2.9.0 in its component *undisclosed* has a ../ directory traversal vulnerability. Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of the restricted directory on the remote server with administrative privileges. Impact: Information Disclosure CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N (<=2.8.9) CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N (<=2.9.0)

7. Administrative Back-door access (CVE-2020-15921)

(Unauthenticated) Mida Solutions eFramework <= 2.9.0 in its component *undisclosed* has a back-door which permits to change the administrative password and access restricted functionalities. Successful exploitation could allow an attacker to access the web application with an administrative account and leverage other vulnerabilities to obtain Code Execution.

- Impact: Privilege Escalation, Code Execution
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

8. Reflected Cross-Site Scripting (XSS) (CVE-2020-15919)

(Unauthenticated) A Reflected Cross Site Scripting (XSS) Vulnerability was discovered in Mida Solutions eFramework <= 2.9.0 component *undisclosed*.

- Impact: Session hijacking
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

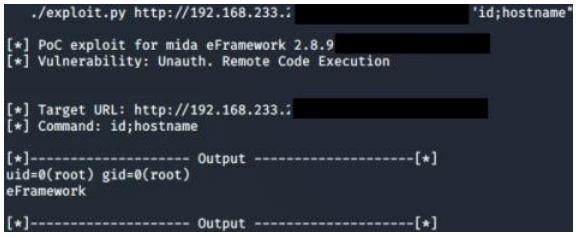
9. Stored XSS (CVE-2020-15918)

(Authenticated) Multiple Stored Cross Site Scripting (XSS) were discovered in Mida Solutions eFramework <= 2.9.0 component *undisclosed*.

- Impact: Session hijacking
- CVSS v3.1 Vector: AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:N/A:N

POC

Complete POC will be released in the next months.



–https://mega.nz/file/yUBX3CSY#4uaS0o6oWGS8yvUxCd8EBQNCc7wAKhMW63bwKEIL6Rg

Vulnerable / tested versions

Mida Solutions eFramework version 2.8.9 has been tested, which was the latest version available at the time of the test. Previous versions may also be affected. In the first quarter of the year the vendor released a newer version 2.9.0. However, the latest version is still vulnerable to the above vulnerabilities.

Vendor response

No response or statement from the vendor.

Vendor contact time-line

- 18/02/2020 e-mail through VSX

- 25/02/2020 e-mail to info@midasolutions.com
- 27/02/2020 e-mail to support@midasolutions.com
- 28/02/2020 e-mail to info@midasolutions.com
- 02/03/2020 chatbot web-site
- 02/03/2020 e-mail to info@midasolutions.com
- 26/03/2020 phone-call to company hq (049**652)
  - > *we are working on it and we will contact you*
- 27/04/2020 e-mail to info@, support@, sales@, mauro.franchin@
- 10/05/2020 e-mail to info@, support@ (with PoC exploit)
- 09/06/2020 report to kb.cert.org
- 01/07/2020 kb.cert.org response received (suggesting public disclosure in around 2 weeks)
  - Public disclosure date (15/07/2020) and draft link reported to info@midasolutions.com
- 08/07/2020 some companies, which are exposing this software on WAN, were notified about the imminent disclosure.
- 15/07/2020 partial public disclosure
- 24/07/2020 CVE assigned

Further information will be released in the next months.
