



ManageEngine AppManager15 (Build No:15510) – DLL Hijacking

Summary



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

Affected versions

AppManager15 (Build No:15510)

Fixed versions

AppManager15 (Build No:15520)

State

Public

Vulnerability

Kind	DLL Hijacking
Rule	<u>413. Insecure file upload - DLL Injection</u>
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CVSSv3 Base Score	9.1
Exploit available	No
CVE ID(s)	<u>CVE-2022-23050</u>



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

Proof of Concept

Steps to reproduce

1. Log in as an admin user.
2. Go to `Settings`.
3. Go to the `Tools` section and click on `Upload Files / Binaries`.
4. Select the `Upload Script` to `<Product_Home>/working/` option.
5. Create a malicious DLL with one of the following names

MSASN1.dll
WTSAPI32.dll
CRYPTSP.dll
CRYPTBASE.dll

6. Upload the file.

7. Go to Shutdown / Restart Service and click on Restart

8. Wait for the service to restart in order to load the DLL file.

System Information

- Version: ManageEngine AppManager15 (Build No:15510).
- Operating System: Windows 10.0.19042 N/A Build 19042.



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

An updated version of ManageEngine is available at the vendor page.

Credits

The vulnerability was discovered by Andrés Roldán and Oscar Uribe from the Offensive Team of Fluid Attacks.

References

**Vendor
page**

<https://www.manageengine.com/>

Release

https://www.manageengine.com/products/applications_manager/

notes

[notes.html](#)

Latest
version

https://www.manageengine.com/products/applications_manager/

Timeline

- ✓ 2022-02-03
Vulnerability discovered.
- ✓ 2022-02-03
Vendor contacted.
- ✓ 2022-02-04
Vendor replied acknowledging the report.



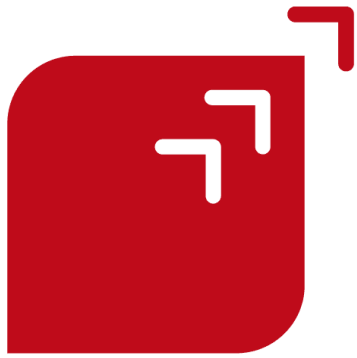
This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

Public Disclosure.



Services



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)[Show details](#)

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

[Service Status](#) - [Terms of Use](#) - [Privacy Policy](#) - [Cookie Policy](#)



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)