



Frappe 14.10.0 - Local File Read

Summary

Frappe 14.10.0 - LFR Name



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

| State | Public |
|--------------|------------|
| Release date | 2022-11-21 |

Vulnerability

| Kind | Lack of data validation - Path Traversal |
|-------------------|---|
| Rule | 063. Lack of data validation - Path Traversal |
| Remote | Yes |
| CVSSv3 Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N |
| CVSSv3 Base Score | 4.3 |
| Exploit available | Yes |
| CVE ID(s) | CVE-2022-41712 |

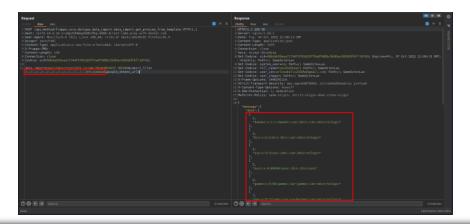
Description

Frappe version 14.10.0 allows an external attacker to remotely obtain arbitrary local files. This is possible because the application does not correctly validate the information injected by the user in the ${\tt import_file}$ parameter.

Vulnerability

This vulnerability occurs because the application does not correctly validate the path of the import file parameter. Thanks to this, an attacker can point to internal server files.

Evidence of exploitation



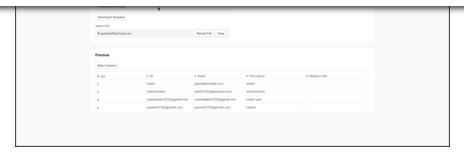
آد

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

Chow dotai



Our security policy

We have reserved the CVE-2022-41712 to refer to this issue from now on.

• https://fluidattacks.com/advisories/policy/

System Information

- Version: Frappe 14.10.0
- Operating System: GNU/Linux

Mitigation

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

Credits

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

References

Vendor page https://github.com/frappe/frappe

Release page https://github.com/frappe/frappe/releases/tag/v14.12.0

Timeline

- 2022-10-10
 Vulnerability discovered.
 2022-10-10
 Vendor contacted.
- 2022-10-10

 Vendor replied acknowledging the report.
- 2022-10-11

 Vendor Confirmed the vulnerability.
- 2022-10-12

≥ 2022-11-21 Public Disclosure.



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

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

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