Server-Side Request Forgery (SSRF) in emissary:emissary

High **drewfarris** published **GHSA-2p8j-2rf3-h4xr** on Jul 2, 2021

Package

emissary:emissary (Maven)

Affected versions	Patched versions
6.4.0	7.0.0

Description

Impact

Emissary is vulnerable to Server-Side Request Forgery (SSRF)

The `RegisterPeerAction` endpoint is vulnerable to Server-Side Request Forgery (SSRF). A POST request to the `/RegisterPeer.action` endpoint will trigger additional requests to hosts controlled by the attacker

Some of the forged requests are non-authenticated requests sent to the `/emissary/Heartbeat.action` endpoint on the attacker server. However, some others are authenticated requests sent to the `/emissary/RegisterPeer.action` endpoint on the attacker-controlled server.

Similarly the `AddChildDirectoryAction` endpoint is vulnerable to Server-Side Request Forgery (SSRF). A POST request to the `/AddChildDirectory.action` endpoint will trigger additional requests to hosts controlled by the attacker:

This vulnerability may lead to credentials leak.

Patches

Has the problem been patched? What versions should users upgrade to?

Workarounds

Disable network access to Emissary from untrusted sources.

References

1. MITRE Common Weakness Enumeration (CWE-918: Server Side Request Forgery)

For more information

If you have any questions or comments about this advisory:

- Open an issue in NationalSecurityAgency/emissary
- Email us at emissarysupport@evoforge.org

Severity

High 7.2 / 10

CVSS base metrics

Attack vector	Network
Attack complexity	High
Privileges required	High
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	Low
Availability	Low

CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:L/A:L

CVE ID

CVE-2021-32639

Weaknesses

CWE-918

Credits

pwntester