



# Server-Side Request Forgery in GitHub Enterprise Server allowed extraction of sensitive environment variables via timing side-channel attack

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-5921
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_P
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 23:16:22 UTC
<b>Updated</b>	2026-04-22 21:23:52 UTC
<b>Description</b>	A server-side request forgery (SSRF) vulnerability was identified in GitHub Enterprise Server that allowed an attacker to ext

## Risk And Classification

**Primary CVSS:** v4.0 8.9 HIGH from product-cna@github.com

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000490000 probability, percentile 0.151090000 (date 2026-04-22)

**Problem Types:** CWE-918 | CWE-918 CWE-918 Server-Side Request Forgery (SSRF)

Version	Source	Type	Score	Severity	Vector
4.0	product-cna@github.com	Secondary	8.9	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L
4.0	CNA	CVSS	8.9	HIGH	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L

## CVSS v4.0 Breakdown

Attack Vector

**Network**

Attack Complexity

**High**

Attack Requirements

**Present**

Privileges Required

**None**

User Interaction

None

Confidentiality

High

Integrity

High

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

Low

CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:L/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">GitHub</a>	<a href="#">Enterprise Server</a>	affected 3.14.0 3.14.26 semver	Not specified
CNA	<a href="#">GitHub</a>	<a href="#">Enterprise Server</a>	affected 3.15.0 3.15.21 semver	Not specified
CNA	<a href="#">GitHub</a>	<a href="#">Enterprise Server</a>	affected 3.16.0 3.16.17 semver	Not specified
CNA	<a href="#">GitHub</a>	<a href="#">Enterprise Server</a>	affected 3.17.0 3.17.14 semver	Not specified
CNA	<a href="#">GitHub</a>	<a href="#">Enterprise Server</a>	affected 3.18.0 3.18.8 semver	Not specified
CNA	<a href="#">GitHub</a>	<a href="#">Enterprise Server</a>	affected 3.19.0 3.19.5 semver	Not specified
CNA	<a href="#">GitHub</a>	<a href="#">Enterprise Server</a>	affected 3.20.0 3.20.1 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="https://docs.github.com/en/enterprise-server@3.18/admin/release-notes">docs.github.com/en/enterprise-server@3.18/admin/release-notes</a>	product-cna@github.com	<a href="https://docs.github.com">docs.github.com</a>	
<a href="https://docs.github.com/en/enterprise-server@3.17/admin/release-notes">docs.github.com/en/enterprise-server@3.17/admin/release-notes</a>	product-cna@github.com	<a href="https://docs.github.com">docs.github.com</a>	
<a href="https://docs.github.com/en/enterprise-server@3.15/admin/release-notes">docs.github.com/en/enterprise-server@3.15/admin/release-notes</a>	product-cna@github.com	<a href="https://docs.github.com">docs.github.com</a>	
<a href="https://docs.github.com/en/enterprise-server@3.14/admin/release-notes">docs.github.com/en/enterprise-server@3.14/admin/release-notes</a>	product-cna@github.com	<a href="https://docs.github.com">docs.github.com</a>	
<a href="https://docs.github.com/en/enterprise-server@3.19/admin/release-notes">docs.github.com/en/enterprise-server@3.19/admin/release-notes</a>	product-cna@github.com	<a href="https://docs.github.com">docs.github.com</a>	
<a href="https://docs.github.com/en/enterprise-server@3.16/admin/release-notes">docs.github.com/en/enterprise-server@3.16/admin/release-notes</a>	product-cna@github.com	<a href="https://docs.github.com">docs.github.com</a>	
<a href="https://docs.github.com/en/enterprise-server@3.20/admin/release-notes">docs.github.com/en/enterprise-server@3.20/admin/release-notes</a>	product-cna@github.com	<a href="https://docs.github.com">docs.github.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA: R31n (en)**

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)