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

CVE	CVE-2026-5921
State	PUBLISHED
Assigner	GitHub_P
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 23:16:22 UTC
Updated	2026-04-22 21:23:52 UTC
Description	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/MSC:X/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/MSC:X/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	GitHub	Enterprise Server	affected 3.14.0 3.14.26 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.15.0 3.15.21 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.16.0 3.16.17 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.17.0 3.17.14 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.18.0 3.18.8 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.19.0 3.19.5 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.20.0 3.20.1 semver	Not specified

References

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

Vendor Comments And Credit

Discovery Credit

CNA: R31n (en)

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