



# Improper authorization fallback allows scoped user-to-server token installation escape in GitHub Enterprise Server

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

## Summary

<b>CVE</b>	CVE-2026-5845
<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>	An improper authorization vulnerability in scoped user-to-server (ghu_) token authorization in GitHub Enterprise Server allo

## Risk And Classification

**Primary CVSS:** v4.0 7.2 HIGH from product-cna@github.com

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N/E:X/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:** 0.000130000 probability, percentile 0.021240000 (date 2026-04-22)

**Problem Types:** CWE-639 | CWE-639 CWE-639 Authorization bypass through User-Controlled key

Version	Source	Type	Score	Severity	Vector
4.0	product-cna@github.com	Secondary	7.2	HIGH	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N/E
4.0	CNA	CVSS	7.2	HIGH	CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:N/SC:L/SI:L/SA:N/E:X/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	GitHub	Enterprise Server	affected 3.20.0 3.20.1 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.19.0 3.19.4 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.18.0 3.18.7 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.17.0 3.17.13 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.16.0 3.16.16 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.15.0 3.15.20 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.14.0 3.14.25 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:** ahacker1 (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](#)