Incorrect Regular Expression vulnerability in GitHub Enterprise Server allowed unauthorized access to user accounts via OAuth callback URL validation bypass

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-4296
State	PUBLISHED
Assigner	GitHub_P
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 23:16:21 UTC
Updated	2026-04-29 12:39:18 UTC
Description	An incorrect regular expression vulnerability was identified in GitHub Enterprise Server that allowed an attacker to bypass C

Risk And Classification

Primary CVSS: v4.0 7.5 HIGH from product-cna@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000500000 probability, percentile 0.154920000 (date 2026-04-22)

Problem Types: CWE-185 | CWE-185 CWE-185 Incorrect Regular Expression

Version	Source	Type	Score	Severity	Vector
4.0	product-cna@github.com	Secondary	7.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/
4.0	CNA	CVSS	7.5	HIGH	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

Passive

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Github	Enterprise Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GitHub	Enterprise Server	affected 3.14.0 3.14.25 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.15.0 3.15.20 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.16.0 3.16.16 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.17.0 3.17.13 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.18.0 3.18.7 semver	Not specified
CNA	GitHub	Enterprise Server	affected 3.19.0 3.19.4 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	Release Notes, Vendor Ad
docs.github.com/en/enterprise-server@3.17/admin/release-notes	product-cna@github.com	docs.github.com	Release Notes, Vendor Ad
docs.github.com/en/enterprise-server@3.15/admin/release-notes	product-cna@github.com	docs.github.com	Release Notes, Vendor Ad
docs.github.com/en/enterprise-server@3.14/admin/release-notes	product-cna@github.com	docs.github.com	Release Notes, Vendor Ad
docs.github.com/en/enterprise-server@3.19/admin/release-notes	product-cna@github.com	docs.github.com	Release Notes, Vendor Ad
docs.github.com/en/enterprise-server@3.16/admin/release-notes	product-cna@github.com	docs.github.com	Release Notes, Vendor Ad
docs.github.com/en/enterprise-server@3.20/admin/release-notes	product-cna@github.com	docs.github.com	Release Notes, Vendor Ad
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)

CNA: hacktron (en)

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