



Denial of service vulnerability in GitHub Enterprise Server allowed service disruption via unauthenticated API endpoint

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2026-7541 |
| State | PUBLISHED |
| Assigner | GitHub_P |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-07 22:16:36 UTC |
| Updated | 2026-05-11 17:19:36 UTC |
| Description | A denial of service vulnerability was identified in GitHub Enterprise Server that allowed an unauthenticated attacker to caus |

Risk And Classification

Primary CVSS: v4.0 6.3 MEDIUM from product-cna@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:U/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 0.150940000 (date 2026-05-12)

Problem Types: CWE-770 | CWE-770 CWE-770 Allocation of resources without limits or throttling

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------|-----------|-------|----------|--|
| 4.0 | product-cna@github.com | Secondary | 6.3 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:U/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 |
| 4.0 | CNA | CVSS | 6.3 | MEDIUM | CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:U/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 |
| 3.1 | nvd@nist.gov | Primary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H/E:U/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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|------------------------|-----------------------------------|--------------------------------|---------------|
| 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@3.16/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 |
| 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@3.19/admin/release-notes | product-cna@github.com | docs.github.com | Release Notes, Vendor Ad |
| docs.github.com/en/enterprise-server@3.18/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: Nguyen Nhat Anh (GitHub: anh2025) (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