



Server-side request forgery vulnerability in GitHub Enterprise Server notebook viewer via URL parser confusion

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-8034 |
| State | PUBLISHED |
| Assigner | GitHub_P |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-05-07 22:16:37 UTC |
| Updated | 2026-05-07 22:16:37 UTC |
| Description | A server-side request forgery (SSRF) vulnerability was identified in the GitHub Enterprise Server notebook viewer that allow |

Risk And Classification

Primary CVSS: v4.0 7.9 HIGH from product-cna@github.com

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

Problem Types: CWE-436 | CWE-918 | CWE-918 CWE-918 Server-Side request forgery (SSRF) | CWE-436 CWE-436 Interpretation Conflict

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------|-----------|-------|----------|---|
| 4.0 | product-cna@github.com | Secondary | 7.9 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H |
| 4.0 | CNA | CVSS | 7.9 | HIGH | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H |

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSG: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 3.16.0 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 |
| CNA | GitHub | Enterprise Server | unaffected 3.21.0 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 | |
| docs.github.com/en/enterprise-server@3.20/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@3.19/admin/release-notes | product-cna@github.com | docs.github.com | |
| docs.github.com/en/enterprise-server@3.18/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.

© [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](#)