21 April 2025

SECURITY ADVISORY
CVE-2025-3509, CVE-2025-3124, & CVE-2025-3246

Telah ditemukan tiga kerentanan yang menargetkan GitHub Enterprise. **CVE-2025-3509** memungkinkan penyerang dengan akses administratif atau kontrol atas ***pre-receive hook*** dapat mengeksekusi kode arbitrer di server yang berpotensi menyebabkan eskalasi hak akses dan kompromi sistem. **CVE-2025-3124** memungkinkan pengguna tanpa izin dapat melihat nama repositori *private* melalui fitur ***Security Overview***, khususnya saat **filter "only *archived*:"** digunakan. Sementara itu, **CVE-2025-3246** memungkinkan penyisipan *malicious script* dalam **blok matematika ($$..$$)** di Markdown yang dapat dieksekusi saat dibuka oleh pengguna.

Nilai/Tingkat

8.2

High

CWE 79 **Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')**

Kerentanan yang muncul ketika input pengguna tidak disaring atau disanitasi dengan benar sebelum ditampilkan di halaman web, memungkinkan penyerang menyisipkan *malicious script* yang menyebabkan terjadinya *Cross-Site-Scripting*.

CWE 94 **Improper Control of Generation of Code ('Code Injection')**

Kerentanan ini terjadi ketika sistem memungkinkan pengguna menyisipkan atau memodifikasi kode yang kemudian dieksekusi tanpa validasi yang memadai.

CWE 200 **Exposure of Sensitive Information to an Unauthorized Actor**

Kerentanan ini terjadi ketika sistem gagal membatasi akses ke data sensitif, seperti nama repositori *private* sehingga pengguna yang tidak berwenang dapat mengakses informasi tersebut.

Langkah Mitigasi

Melakukan pembaruan GitHub Enterprise Server ke versi terbaru yang telah dilakukan patching keamanan untuk menutup kerentanan tersebut.

Produk Terancam

- GitHub Enterprise Server Versi 3.16.1.
- GitHub Enterprise Server Versi < 3.17.

Referensi Lanjutan, Solusi, dan Alat

- https://nvd.nist.gov/vuln/detail/cve-2025-3509
- https://nvd.nist.gov/vuln/detail/cve-2025-3124
- https://nvd.nist.gov/vuln/detail/cve-2025-3246

Informasi Imbauan Keamanan Lainnya di laman **Id-SIRTII/CC**

https://www.idsirtii.or.id/peringatan.html

Sumber Penulisan

- [Diakses 21 April 2025] https://securityonline.info/github-enterprise-server-vulnerabilities-expose-risk-of-code-execution-and-data-leaks

Diterbitkan Oleh

Id-SIRTII/CC

Indonesia Security Incident Response team on Internet Infrastructure Coordination Center

Badan Siber dan Sandi Negara

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan, Pasar Minggu, Jakarta Selatan 12550