

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

**Patch Now: Critical Auth Bypass Flaw
in GitHub Enterprise Server Fixed**

Date of Publication

May 23, 2024

Admiralty Code

A1

TA Number

TA2024202




Summary

First Seen: May 21, 2024

Affected Product: GitHub Enterprise Server (GHES)

Impact: CVE-2024-4985 is a critical severity vulnerability that affects GitHub Enterprise Server (GHES). It allows an attacker to bypass authentication and gain access to a GHES instance, potentially with site administrator privileges, without requiring pre-authentication.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-4985	GitHub Enterprise Server Authentication Bypass Vulnerability	GitHub Enterprise Server (GHES)			

Vulnerability Details

#1

A critical authentication bypass vulnerability, CVE-2024-4985, with a maximum severity (CVSS V4 Score: 10.0), was recently fixed by GitHub. This vulnerability impacts GitHub Enterprise Server (GHES) instances employing SAML single sign-on (SSO) authentication, particularly those utilizing the optional encrypted assertions feature.

#2

The vulnerability exists because of the way GHES handles encrypted SAML claims with Single Sign-On (SSO) authentication. An attacker can forge a fake SAML claim that appears valid to GHES, granting them unauthorized access.

#3

GHEE is a self-hosted version of GitHub for organizations needing more control over their repositories, often due to confidentiality, high performance requirements, or offline access needs.

#4

To mitigate potential security threats, users are advised to update to the latest version of GHEE, especially since a proof-of-concept (PoC) exploit for the vulnerability has been released. If you cannot upgrade immediately, consider disabling the optional encrypted assertions feature in SAML SSO.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4985	All versions of GitHub Enterprise Server prior to 3.13.0	cpe:2.3:a:github:enterprise_server:*:*:*:*:*	CWE-303

Recommendations



Apply Patch: Update your GitHub Enterprise Server (GHEE) instances to the latest fixed versions: 3.12.4, 3.11.10, 3.10.12, or 3.9.15. This is the most effective way to mitigate the vulnerability.



Verify SAML Configuration: Ensure that your SAML single sign-on (SSO) configurations are correctly set up and that encrypted assertions are being used as intended. Misconfigurations can increase the risk of exploitation.



Monitor Activity: Regularly monitor and audit GHEE access logs and activities for any unusual or unauthorized access attempts. Early detection of suspicious activity can help mitigate potential breaches.



Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

<u>TA0006</u> Credential Access	<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	<u>T1556</u> Modify Authentication Process
<u>T1606.002</u> SAML Tokens	<u>T1606</u> Forge Web Credentials	<u>T1190</u> Exploit Public-Facing Application	<u>T1068</u> Exploitation for Privilege Escalation

Patch Details

Update to GHES versions 3.12.4, 3.11.10, 3.10.12, 3.9.15 or later

Links:

<https://docs.github.com/en/enterprise-server@3.12/admin/release-notes#3.12.4>

<https://docs.github.com/en/enterprise-server@3.11/admin/release-notes#3.11.10>

<https://docs.github.com/en/enterprise-server@3.10/admin/release-notes#3.10.12>

<https://docs.github.com/en/enterprise-server@3.9/admin/release-notes#3.9.15>

References

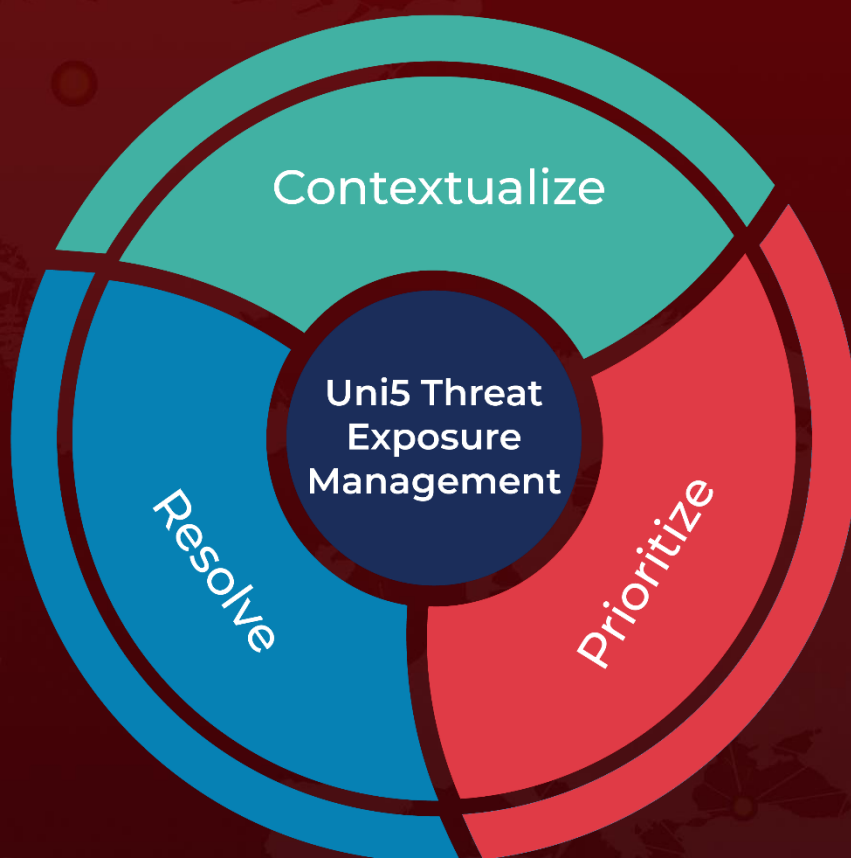
<https://github.com/advisories/GHSA-5pw9-f9r4-mv2r>

<https://github.com/absholi7ly/Bypass-authentication-GitHub-Enterprise-Server>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

May 23, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com