

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

GitHub Addresses Admin Privilege Exploits in Enterprise Server

Date of Publication

August 28, 2024

Admiralty Code

A1

TA Number

TA2024330










Summary

First Seen: August 20, 2024

Affected Product: GitHub Enterprise Server

Impact: GitHub has addressed three critical security vulnerabilities in Enterprise Server (GHES), tracked as CVE-2024-6800, CVE-2024-6337, and CVE-2024-7711. These flaws could enable attackers to bypass normal login processes and gain high-level access by exploiting weaknesses in how the system validated the security of login tokens.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-6800	GitHub SAML Token Forgery Vulnerability	GitHub Enterprise Server			
CVE-2024-6337	GitHub Unauthorized Data Disclosure Vulnerability	GitHub Enterprise Server			
CVE-2024-7711	GitHub Unauthorized Public Repository Issue Updates	GitHub Enterprise Server			

Vulnerability Details

#1

GitHub has addressed three critical security vulnerabilities in Enterprise Server (GHES), identified as CVE-2024-6800, CVE-2024-6337, and CVE-2024-7711. These vulnerabilities could allow attackers to gain unauthorized access and manipulate repositories. There are over 36,500 GHES instances exposed on the public web, with approximately 29,200 of these located in the United States.

#2

CVE-2024-6800 pertains to a flaw in the processing of SAML responses, the security tokens used for user authentication. The vulnerability specifically affected the XML signature within the token, which ensures its integrity. Exploiting this weakness, an attacker could forge a SAML response, granting them unauthorized entry to sensitive areas of the system, such as administrator accounts, without requiring valid login credentials.

#3

The other vulnerabilities include CVE-2024-7711, which could allow an attacker to modify the title, assignees, and labels of issues in public repositories, though private and internal repositories are not affected. CVE-2024-6337 could enable an attacker to view issue content in a private repository via a GitHub App with limited read and write permissions.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-6800	GitHub Enterprise Server versions: 3.13.0 through 3.13.2, 3.10.0 through 3.10.15, 3.11.0 through 3.11.13, 3.12.0 through 3.12.7	cpe:2.3:a:github:enterprise_server:*:*:*:*:*:*:*	CWE-347
CVE-2024-6337	GitHub Enterprise Server versions: 3.13.0 through 3.13.2, 3.10.0 through 3.10.15, 3.11.0 through 3.11.13, 3.12.0 through 3.12.7		CWE-863
CVE-2024-7711	GitHub Enterprise Server versions: 3.13.0 through 3.13.2, 3.11.0 through 3.11.13, 3.12.0 through 3.12.7		CWE-863

Recommendations



Upgrade to Supported Versions: Organizations using GitHub Enterprise Server version 3.10 should plan to upgrade to a newer version before August 29, 2024. As version 3.10 will be discontinued and will no longer receive patches or security fixes, upgrading to a supported version ensures continued access to security updates and new features.



Prioritize Critical Updates: Ensure that all instances of GitHub Enterprise Server are updated to the latest versions that address the identified vulnerabilities (CVE-2024-6800, CVE-2024-6337, and CVE-2024-7711). Specifically, update to GitHub Enterprise Server versions 3.13.3, 3.10.16, 3.11.14, or 3.12.8, as these versions include patches for the critical security issues.



Review and Harden Configuration Settings: Perform periodic security audits of GitHub Enterprise Server configurations to identify and address potential weaknesses. Review and adjust default settings to enhance security, including disabling unnecessary features and services.



Regularly Review and Update Dependencies: Monitor and update any third-party integrations or dependencies used with the GitHub Enterprise Server. Ensure that these components are also kept up-to-date with security patches to avoid potential vulnerabilities.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0040 Impact
T1213 Data from Information Repositories	T1134.003 Make and Impersonate Token	T1078 Valid Accounts	T1059 Command and Scripting Interpreter
T1212 Exploitation for Credential Access	T1565 Data Manipulation	T1565.001 Stored Data Manipulation	T1068 Exploitation for Privilege Escalation

Patch Details

GitHub has addressed all three critical security vulnerabilities with the release of the following GitHub Enterprise Server (GHES) versions:

- **3.13.3**
- **3.12.8**
- **3.11.14**
- **3.10.16**

These updates patch the identified vulnerabilities and enhance the overall security of the GHES environment.

Links:

<https://docs.github.com/en/enterprise-server@3.10/admin/release-notes#3.10.16>

<https://docs.github.com/en/enterprise-server@3.11/admin/release-notes#3.11.14>

<https://docs.github.com/en/enterprise-server@3.12/admin/release-notes#3.12.8>

<https://docs.github.com/en/enterprise-server@3.13/admin/release-notes#3.13.3>

References

<https://docs.github.com/en/enterprise-server@3.13/admin/release-notes#3.13.2-security-fixes>

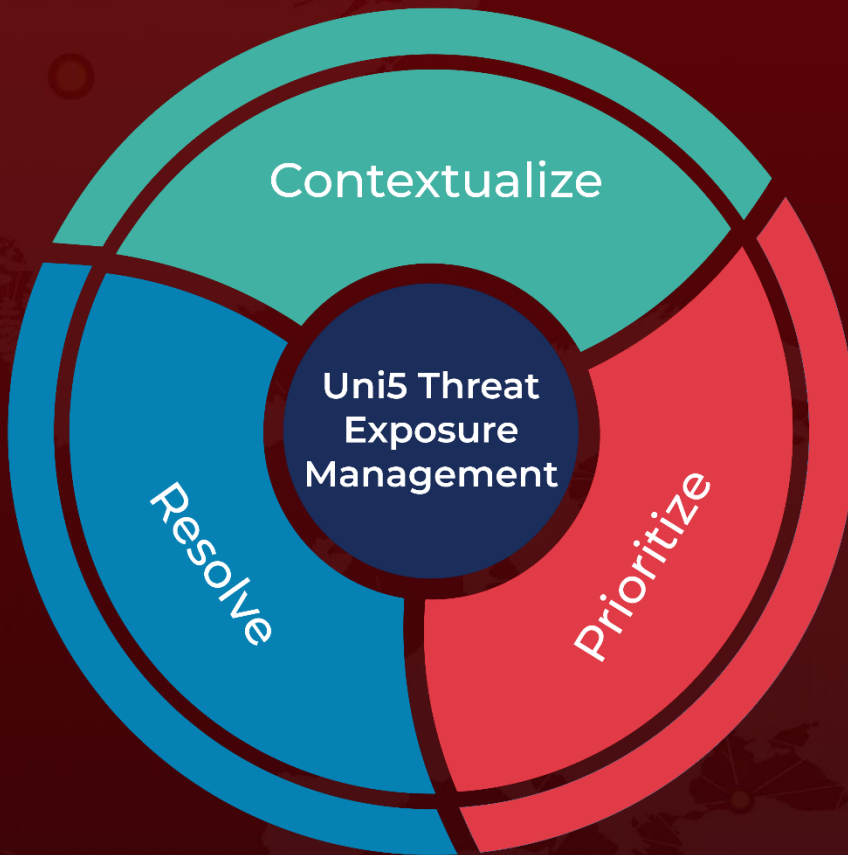
<https://threatprotect.qualys.com/2024/08/21/github-patches-multiple-security-vulnerabilities-cve-2024-6800-cve-2024-6337-cve-2024-7711/>

<https://cyble.com/blog/saml-exploit-github-cve-2024-6800/>

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

August 28, 2024 • 3:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com