مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Imperva SecureSphere WAF

Tracking #:432315745

Date:02-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability in Imperva SecureSphere WAF, a popular on-premise Web Application Firewall (WAF).

TECHNICAL DETAILS:

This vulnerability, identified as **CVE-2023-50969**, has a **CVSS score of 9.8**,which means it is extremely severe. It allows attackers to bypass security protocols designed to protect against common web attacks, such as SQL injection and cross-site scripting (XSS).

Here's a summary of the vulnerability:

Impacted product: Imperva SecureSphere WAF
CVE ID: CVE-2023-50969
Severity: Critical (CVSS score: 9.8)
Impact: Allows attackers to bypass security rules and launch attacks on protected applications.

Affected Versions:

- Imperva SecureSphere WAF v14.7.0.40 and earlier versions are susceptible.
- Imperva Cloud WAF is not affected.

Fixed Version(s):

- As Per Imperva, this issue can be remediated by an ADC rule update that was released on February 26, 2024. Imperva customers may get more information by logging into the Imperva Support Portal and reviewing the following document: https://docs.imperva.com/bundle/z-kb-articles-km/page/f81a5705.html

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update to the latest version and Conduct a comprehensive audit of web applications.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

1. https://www.hoyahaxa.com/2024/03/imperva-waf-bypass-cve-2023-50969.html