FORTINET

OUTBREAK ALERTS

Microsoft SharePoint Server Elevation of Privilege Vulnerability

Actively targeted in the wild

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357
CVEs: CVE-2023-29357

CVE-2023-29357 is an authentication bypass vulnerability, which means that adversaries may use it to escalate privileges on affected installations of Microsoft SharePoint Server. If the user is a privileged account, such as an administrator, the attacker will gain elevated privileges.

Background

This vulnerability stems from the validation check used to verify JSON Web Tokens (JWTs) used for authentication. An attacker who has gained access to spoofed JWT authentication tokens can use them to bypasses authentication and gain access to the privileges of an authenticated user.

Attackers may chain CVE-2023-29357 vulnerability with other vulnerabilities for remote code execution to compromise the integrity, availability, and confidentiality of the target system.

Announced

Jun 13, 2023: Microsoft released the advisory and patch guide for the vulnerability (CVE-2023-29357)
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29357

Latest Developments

Jan 1, 2024: CISA added CVE-2023-29357 to its known exploited catalog.

Fortinet customers remain protected via the IPS signature service and can detect vulnerable SharePoint servers to CVE-2023-29357. IPS signature has been released since June, 2023 to protect and detect any attack attempts, however users are recommended to apply patches to the vulnerable systems as soon as possible to mitigate any risks if not already done.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Weaponization

Delivery

Vulnerability

Detect vulnerable SharePoint Servers (CVE-2023-29357)

- FortiClient — *DB 1.48*

Exploitation

IPS

Detect and block attack targeting sharePoint Servers (CVE-2023-29357)

- FortiGate — *DB 25.637*
- FortiSASE — *DB 25.637*
- FortiNDR — *DB 25.637*
- FortiADC — *DB 25.637*
- FortiProxy — *DB 25.637*

Installation

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

- FortiAnalyzer — *DB 2.00033*
- FortiSIEM — *DB 603*

Threat Hunting

- FortiAnalyzer — *v6.4+*

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

- FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

- Incident Response
- FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

- NSE Training
- Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

- Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

- Security Rating

Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

- FortiClient

Business Reputation

Know attackers next move to protect against your business branding.

- FortiRecon: EASM

Additional Resources

Bleeping Computer https://www.bleepingcomputer.com/news/security/exploit-released-for-microsoft-sharepoint-server-auth-bypass-flaw/

Dark Reading https://www.darkreading.com/vulnerabilities-threats/researchers-release-details-of-new-rce-exploit-chain-for-sharepoint

Learn more about FortiGuard Outbreak Alerts

FORTINET