مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Fortinet

Tracking #:432316502

Date:13-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Fortinet has released security updates to address multiple vulnerabilities affecting FortiOS, FortiClient, FortiAnalyzer, and FortiManager products. These vulnerabilities could potentially be exploited to hijack user sessions, bypass authentication, escalate privileges, and execute arbitrary code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

1. **CVE-2023-50176 (FortiOS)**
   - CVSS v3 Score: 7.1 (High)
   - A session fixation vulnerability that may allow an unauthenticated attacker to hijack user sessions via a phishing SAML authentication link
2. **CVE-2024-47574 (FortiClient Windows)**
   - CVSS v3 Score: 7.4 (High)
   - An authentication bypass vulnerability that may allow a low-privilege attacker to execute arbitrary code with high privileges via spoofed named pipe messages
3. **CVE-2024-36513 (FortiClient Windows)**
   - CVSS v3 Score: 7.4 (High)
   - A privilege context switching error that may allow an authenticated user to escalate their privileges via lua auto patch scripts
4. **CVE-2024-23666 (FortiAnalyzer)**
   - CVSS v3 Score: 7.1 (High)
   - Details not provided in the given information.
5. **CVE-2024-36513 (FortiAnalyzer)**
   - CVSS v3 Score: 7.4 (High)
   - A client-side enforcement of server-side security vulnerability that may allow an authenticated attacker with at least read-only permission to execute sensitive operations via crafted requests

Version	Affected Versions	Fixed Versions
FortiOS 7.4	7.4.0 through 7.4.3	Upgrade to 7.4.4 or above
FortiOS 7.2	7.2.0 through 7.2.7	Upgrade to 7.2.8 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiClientWindows 7.4	7.4.0	Upgrade to 7.4.1 or above
FortiClientWindows 7.2	7.2.0 through 7.2.4	Upgrade to 7.2.5 or above
FortiClientWindows 7.0	7.0.0 through 7.0.12	Upgrade to 7.0.13 or above
FortiClientWindows 6.4	6.4 all versions	Migrate to a fixed release
FortiAnalyzer 7.4	7.4.0 through 7.4.1	Upgrade to 7.4.3 or above
FortiAnalyzer 7.2	7.2.0 through 7.2.4	Upgrade to 7.2.6 or above
FortiAnalyzer 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.13 or above
FortiAnalyzer 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiAnalyzer-BigData 7.4	7.4.0	Upgrade to 7.4.1 or above
FortiAnalyzer-BigData 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiAnalyzer-BigData 7.0	7.0 all versions	Migrate to a fixed release
FortiAnalyzer-BigData 6.4	6.4 all versions	Migrate to a fixed release

FortiAnalyzer-BigData 6.2	6.2 all versions	Migrate to a fixed release
FortiManager 7.4	7.4.0 through 7.4.1	Upgrade to 7.4.3 or above
FortiManager 7.2	7.2.0 through 7.2.4	Upgrade to 7.2.6 or above
FortiManager 7.0	7.0.0 through 7.0.11	Upgrade to 7.0.13 or above
FortiManager 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-144
- https://fortiguard.fortinet.com/psirt/FG-IR-23-396
- https://fortiguard.fortinet.com/psirt/FG-IR-24-199
- https://fortiguard.fortinet.com/psirt/FG-IR-23-475