مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple High-Severity Vulnerabilities in Fortinet products

Tracking #:432316967
Date:13-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity vulnerabilities in Fortinet products. These vulnerabilities could allow unauthorized access, code execution, information disclosure, and other malicious activities on affected systems.

TECHNICAL DETAILS:

High-Severity Vulnerabilities:

- **CVE-2023-48790: FortiNDR Cross-Site Request Forgery (CSRF)**
  - **Description:** A CSRF vulnerability in FortiNDR allows a remote, unauthenticated attacker to execute unauthorized actions via crafted HTTP GET requests.
  - **Impact:** Unauthorized actions on the FortiNDR appliance.
- **CVE-2023-40723: FortiSIEM Sensitive Information Disclosure**
  - **Description:** An exposure of sensitive information vulnerability in FortiSIEM allows a remote, unauthenticated attacker who has obtained the agent's authorization header through other means to read the database password via crafted API requests.
  - **Impact:** Disclosure of sensitive database credentials.
- **CVE-2024-45328: FortiSandbox Incorrect Authorization**
  - **Description:** An incorrect authorization vulnerability in FortiSandbox allows a low-privileged administrator to execute elevated CLI commands via the GUI console menu.
  - **Impact:** Privilege escalation.
- **CVE-2024-55590: FortiIsolator OS Command Injection**
  - **Description:** Multiple OS command injection vulnerabilities in FortiIsolator allow an authenticated attacker with at least read-only admin permission and CLI access to execute unauthorized code via crafted CLI commands.
  - **Impact:** Remote code execution.
- **CVE-2024-45324: FortiOS, FortiProxy, FortiPAM, FortiSRA, FortiWeb Format String Vulnerability**
  - **Description:** A use of externally-controlled format string vulnerability in FortiOS, FortiProxy, FortiPAM, FortiSRA, and FortiWeb allows a privileged attacker to execute unauthorized code or commands via specially crafted HTTP or HTTPS commands.
  - **Impact:** Remote code execution.
- **CVE-2024-52961: FortiSandbox OS Command Injection**
  - **Description:** An improper neutralization of special elements used in an OS Command vulnerability in FortiSandbox allows an authenticated attacker with at least read-only permission to execute unauthorized commands via crafted requests.
  - **Impact:** Unauthorized command execution.
- **CVE-2024-54027: FortiSandbox Hard-coded Cryptographic Key**
  - **Description:** A use of hard-coded cryptographic key vulnerability in FortiSandbox allows a privileged attacker with super-admin profile and CLI access to read sensitive data via CLI.
  - **Impact:** Sensitive data disclosure.
- **CVE-2023-37933: FortiADC Cross-Site Scripting (XSS)**
  - **Description:** An improper neutralization of input during web page generation (XSS) vulnerability in the FortiADC GUI allows an authenticated attacker to perform an XSS attack via crafted HTTP or HTTPS requests.

- **Impact:** Cross-site scripting attacks, potentially leading to session hijacking or other malicious actions.

Note: Refer to the Fortinet advisory for affected and fixed versions, and further details.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Fortinet.

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-23-353
- https://fortiguard.fortinet.com/psirt/FG-IR-23-117
- https://fortiguard.fortinet.com/psirt/FG-IR-24-261
- https://fortiguard.fortinet.com/psirt/FG-IR-24-178
- https://fortiguard.fortinet.com/psirt/FG-IR-24-325
- https://fortiguard.fortinet.com/psirt/FG-IR-24-306
- https://fortiguard.fortinet.com/psirt/FG-IR-24-327
- https://fortiguard.fortinet.com/psirt/FG-IR-23-216