MS-ISAC® Cybersecurity Advisory

TLP:CLEAR
MS-ISAC CYBERSECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2023-028 - **UPDATED**

DATE(S) ISSUED:
03/08/2023
03/14/2023 - UPDATED

SUBJECT:
Multiple Vulnerabilities in Fortinet Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Fortinet Products, the most severe of which could allow for arbitrary code execution. Fortinet has several products that are able to deliver high-performance network security solutions that protect your network, users, and data from continually evolving threats.

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the affected service account. Depending on the privileges associated with the service account an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Service accounts that are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

March 14th – UPDATED THREAT INTELLEGENCE:
Multiple open sources are reporting government entities and large organizations have been targeted by an unknown threat actor exploiting a security flaw in

Fortinet FortiOS software. This targeting has resulted in data loss and OS and file corruption. This is specifically related to a zero-day flaw (CVE-2022-41328), a medium security path traversal bug in FortiOS that could lead to arbitrary code execution.

SYSTEMS AFFECTED:

- FortiAnalyzer version prior to 7.2.2
- FortiAuthenticator version prior to 6.5.0
- FortiDeceptor version prior to 3.2.0
- FortiMail version prior to 6.4.1
- FortiManager version prior to 6.0.5
- FortiPortal version prior to 6.0.10
- FortiSwitch version prior to 7.0.5
- FortiNAC version prior to 9.4.2
- FortiOS version prior to 7.2.4
- FortiProxy version prior to 7.2.2
- FortiRecorder version prior to 7.0.0
- FortiSOAR version prior to 7.3.2
- FortiWeb version prior to 7.2.0

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Fortinet Products, the most severe of

which could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

Tactic: *Initial Access* (TA0001):

Technique: *Exploit Public Facing Application* (T1190):

- CVE-2023-25610 – FortiOS / FortiProxy – Heap buffer underflow in administrative interface: administrative interface may allow a remote unauthenticated attacker to execute arbitrary code on the device and/or perform a DoS on the GUI
- CVE-2022-39951 - FortiWeb - command injection in webserver: An improper neutralization of special elements used in an OS command vulnerability in FortiWeb may allow authenticated users to execute unauthorized code or commands via specifically crafted HTTP requests.
- CVE-2022-39953 - FortiNAC - Multiple privilege escalation via sudo command: An improper privilege management vulnerability in FortiNAC may allow a low privilege local user with shell access to execute arbitrary commands as root.
- CVE-2022-40676 - FortiNAC - Multiple Reflected XSS: An improper neutralization of input during web page generation in FortiNAC may allow an authenticated user to perform an XSS attack via crafted HTTP requests.
- CVE-2023-25605 - FortiSOAR - Improper Authorization in request headers: An improper access control vulnerability in FortiSOAR's playbook component may allow an attacker authenticated on the administrative interface to perform unauthorized actions via crafted HTTP requests.
- CVE-2022-42476 - FortiOS / FortiProxy - Path traversal vulnerability allows VDOM escaping: A relative path traversal vulnerability in FortiOS and FortiProxy may allow privileged VDOM administrators to escalate their privileges to super admin of the box via crafted CLI requests.

Details of lower-severity vulnerabilities are as follows:

- CVE-2023-25611 - FortiAnalyzer - CSV injection in macro name
- CVE-2023-23776 - FortiAnalyzer -- the log-fetch client request password is shown in clear text in the heartbeat response
- CVE-2022-29056 - FortiAuthenticator, FortiDeceptor & FortiMail - Improper restriction over excessive authentication attempts
- CVE-2022-27490 - FortiManager, FortiAnalyzer, FortiPortal & FortiSwitch - Information disclosure through diagnose debug commands
- CVE-2022-45861 - FortiOS & FortiProxy - Access of NULL pointer in SSLVPNd

- CVE-2022-41328 - FortiOS - Path traversal in execute command
- CVE-2022-41329 - FortiOS / FortiProxy - Unauthenticated access to static files containing logging information
- CVE-2022-41333 - FortiRecorder - DoS in login authentication mechanism
- CVE-2022-22297 - FortiWeb and FortiRecorder - Arbitrary file read through command line pipe

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the context of the affected service account. Depending on the privileges associated with the service account an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Service accounts that are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate updates provided by FortiNet to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.3: Perform Automated Operating System Patch Management:** Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of

externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.

- **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
- **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
- **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
- **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.

- Vulnerability scanning is used to find potentially exploitable software vulnerabilities to remediate them. (**M1016: Vulnerability Scanning)**
    - **Safeguard 16.13: Conduct Application Penetration Testing:** Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing.Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
    - **Safeguard 5.5: Establish and Maintain an Inventory of Service Accounts:** Establish and maintain an inventory of service accounts. The inventory, at a minimum, must contain department owner, review date, and purpose. Perform service account reviews to validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.
    - **Safeguard 6.8: Define and Maintain Role-Based Access Control:** Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.
- Architect sections of the network to isolate critical systems, functions, or resources. Use physical and logical segmentation to prevent access to potentially sensitive systems and information. Use a DMZ to contain any internet-facing services that should not be exposed from the internal network. Configure separate virtual private cloud (VPC) instances to isolate critical cloud systems. (**M1030: Network Segmentation)**
    - **Safeguard 12.2: Establish and Maintain a Secure Network Architecture:** Establish and maintain a secure network architecture. A

secure network architecture must address segmentation, least privilege, and availability, at a minimum.

- Restrict execution of code to a virtual environment on or in transit to an endpoint system. (**M1048: Application Isolation and Sandboxing**)
    - **Safeguard 16.8: Separate Production and Non-Production Systems:** Maintain separate environments for production and non-production systems.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.
- Restrict use of certain websites, block downloads/attachments, block Javascript, restrict browser extensions, etc. (**M1021: Restrict Web-Based Content**)
    - **Safeguard 9.2: Use DNS Filtering Services:** Use DNS filtering services on all enterprise assets to block access to known malicious domains.
    - **Safeguard 9.3: Maintain and Enforce Network-Based URL Filters:** Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.
    - **Safeguard 9.6: Block Unnecessary File Types:** Block unnecessary file types attempting to enter the enterprise's email gateway.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources. Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources. (**M1017: User Training**)
    - **Safeguard 14.1: Establish and Maintain a Security Awareness Program:** Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and

update content annually, or when significant enterprise changes occur that could impact this Safeguard.

- **Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:** Train workforce members to recognize social engineering attacks, such as phishing, pre-texting, and tailgating.

REFERENCES:

Fortinet:

https://www.fortiguard.com/psirt?date=03-2023

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22297
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27490
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29056
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39951
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39953
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40676
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41328
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41329
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41333
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42476
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25605
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25611

March 14th – UPDATED REFERENCES:

BleepingComputer:

https://www.bleepingcomputer.com/news/security/fortinet-new-fortios-bug-used-as-zero-day-to-attack-govt-networks/

Multi-State Information Sharing and Analysis Center (MS-ISAC)
Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
31 Tech Valley Drive
East Greenbush, NY 12061

24×7 Security Operations Center
SOC@cisecurity.org - 1-866-787-4722

TLP:CLEAR

www.cisa.gov/tlp

Information may be distributed without restriction, subject to standard copyright rules.

Center for Internet Security

Northeast Headquarters | 31 Tech Valley Drive | East Greenbush, NY 12061 | Phone: 518-266-3460