THREAT ADVISORY

July 18, 2023

A Vulnerability in FortiOS and FortiProxy Could Allow for Remote Code Execution

OVERVIEW

A vulnerability has been discovered in Fortinet FortiOS and FortiProxy, which could allow for remote code execution. FortiOS is the Fortinet's proprietary Operation System which is utilized across multiple product lines. FortiProxy is a secure web gateway that attempts to protects users against internet-borne attacks, and provides protection and visibility to the network against unauthorized access and threats. Successful exploitation of this vulnerability could allow for remote 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.

SYSTEMS AFFECTED

- FortiOS version 7.2.0 through 7.2.3
- FortiOS version 7.0.0 through 7.0.10
- FortiProxy version 7.2.0 through 7.2.2
- FortiProxy version 7.0.0 through 7.0.9

RISK

Government:

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

Businesses:

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

Homes: Low

TECHNICAL SUMMARY

A vulnerability has been discovered in Fortinet FortiOS and FortiProxy, which could allow for remote code execution. Details of the vulnerability are as follows:

Tactic: *Initial Access (*TA0001):

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

- CVE-2023-33308 - A stack-based overflow vulnerability in FortiOS & FortiProxy may allow a remote attacker to execute arbitrary code or command via crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection.

Successful exploitation of this vulnerability could allow for remote 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 7.4: 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.
- Utilize vulnerability scanning 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.

REFERENCES

- **Fortinet:** https://www.fortiguard.com/psirt/FG-IR-23-183
- **CVE:** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33308