Fortinet API Endpoint Detection

Updated : 11/19/2025

Contributors

John Lampe - Author

Overview

As enterprise networks increasingly rely on API-driven infrastructure, Fortinet devices have become high-value targets for attackers seeking to exploit misconfigurations, unpatched vulnerabilities, or exposed administrative interfaces. This plugin provides proactive, protocol-aware detection of access to sensitive Fortinet API endpoints — many of which are tied to configuration, diagnostics, and command execution.

By monitoring for high-risk endpoints we hope to reap the benefits of:

- **Early detection of reconnaissance and exploitation attempts**, including CVEs like CVE-2025-58034
- **Visibility into unauthorized or anomalous API usage**, especially POST-based actions that modify system state
- **Coverage for both authenticated and unauthenticated probes**, reducing dwell time and improving incident response
- **Support for threat hunting and forensic correlation**, by logging endpoint access patterns and payloads

Endpoints In Scope

Endpoint	HTTP Methods	Information
/api/v2/monitor/system/status	GET	Reveals system health, firmware version, and uptime — useful for fingerprinting
/api/v2/cmdb/system/admin	GET, POST, PUT, DELETE	Exposes or modifies admin accounts — risk of privilege escalation or account takeover
/api/v2/cmdb/firewall/address	GET, POST, PUT, DELETE	Discloses internal IP ranges — aids lateral movement and targeting

/api/v2/cmdb/firewall/policy	GET, POST, PUT, DELETE	Reveals firewall rules — attackers can identify weak or overly permissive policies
/api/v2/monitor/log/device	GET, POST	Grants access to logs — may expose credentials, attack traces, or sensitive data
/api/v2/monitor/system/config/backup	POST	Triggers config export — may leak credentials, VPN keys, and full device configuration
/api/v2/monitor/system/firmware	GET, POST	Reveals firmware version or initiates upgrade — exploitable if unpatched
/api/v2/monitor/system/cli	POST	Executes CLI commands via API — high-risk vector for command injection (e.g., CVE-2025-58034)

Goals

- Detect when and how Fortinet API endpoints are being queried
- Use as a starting point for finding
    - Information Leakage
    - Privilege Escalation
    - Remote Code Execution
    - Frequency of attacks
    - Discovered Threats

Stakeholders

- Internal Trinity Cyber Hunters and Devs
- Our clients

Existing Solution

There are no existing Discovery Formulas for Fortinet. There are 13 Threat Formulas, but they are specific to a particular CVE.

Open Questions

None at the moment

Context Engines to be used

- HTTPRequest Context Engine
    - canonical_uri_parts_path_regex
- Meta Context Engine
    - Trust_initiated : false

Code to be reviewed

Attached in separate file