SOLUTION BRIEF

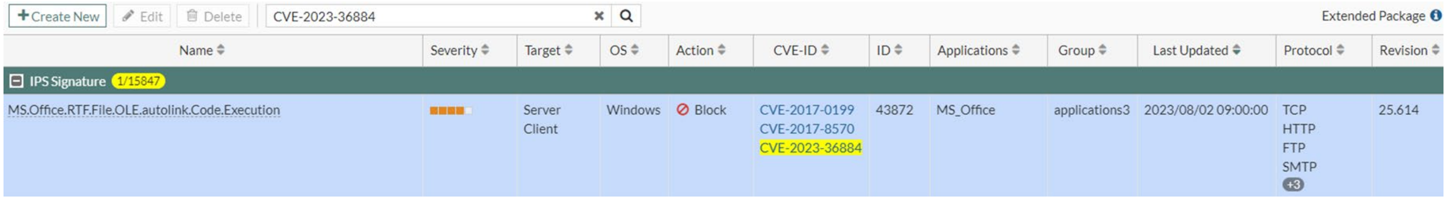
Signature Clustering: A Powerful IPS Feature You Should Be Using

Executive Summary

FortiGuard IPS provides advanced real-time threat detection and prevention capabilities designed to safeguard IT and OT organizations against a wide range of cyberthreats, including zero-day attacks. Of course, most security professionals understand the fundamentals of IPS technologies. But there is one feature of the FortiGuard IPS solution they may not be familiar with—signature clustering. This function helps consolidate and manage all signatures related to a specific vulnerability or threat, thereby enhancing accuracy in identifying, managing, and mitigating security risks while simultaneously making the system more efficient.

How Signature Clustering Works

- **Reduce false positives:** By consolidating similar signatures into clusters, organizations can drastically reduce false positives, minimizing the chances of legitimate traffic being flagged as malicious, thereby avoiding risks and unnecessary disruptions to business operations.
- **Optimize performance:** Clustering similar signatures optimizes the processing efficiency of FortiGuard IPS. It frees up processor bandwidth, enables effective resource utilization, and ensures better performance, even in high-traffic environments, without compromising security effectiveness.
- **Better signature management:** Rather than handling individual signatures, signature clustering simplifies signature management for analysts, thereby allowing them to focus on managing and updating signature clusters, resulting in saved time and effort.
- **Improved accuracy:** FortiGuard IPS uses signature clustering to effectively target and manage the various attack vectors linked to a single vulnerability. This holistic strategy elevates the precision of threat detection.



Name	Severity	Target	OS	Action	CVE-ID	ID	Applications	Group	Last Updated	Protocol	Revision
IPS Signature 1/15847											
MS.Office.RTF.File.OLE.autolink.Code.Execution	■■■■□	Server Client	Windows	Block	CVE-2017-0199 CVE-2017-8570 CVE-2023-36884	43872	MS_Office	applications3	2023/08/02 09:00:00	TCP HTTP FTP SMTP +3	25.614

Figure 1: An example of signature clustering

IPS without Signature Clustering

The traditional method of signature management can lead to several challenges, including:

- Alert overload: Without signature clustering, an IPS system may generate numerous alerts for similar or related threats, thereby overwhelming security teams with a high volume of notifications. This can lead to:
  - Alert fatigue
  - Resource drain due to handling duplicate alerts
  - Excessive investigation and ineffective triage that make identifying, prioritizing, and responding to genuine security incidents difficult
  - Inefficient resource allocation

- Reduced accuracy: Multiple alerts for the same attack or campaign may accidentally be treated as separate incidents, leading to inaccuracies in threat identification and response.
- Siloed context: Without clustering, security analysts may not get the entire context of an attack, making it challenging to fully understand an attacker's tactics, techniques, and procedures and ultimately making it harder to develop effective countermeasures.
- Reduced scalability: A high volume of unclustered alerts can impact the performance of an IPS system and affect its scalability.
- No automation of known threats: Without clustering, organizations may miss opportunities to automate containment and response actions for known threats, thereby increasing response times.

Conclusion: Signature Clustering Is Indispensable

Signature clustering is vital for security teams looking to reduce alert fatigue, improve accuracy, streamline investigations, and enable more efficient incident response. A reduced number of signatures does not mean that coverage is lower. It simply means that FortiGuard IPS works more efficiently, quickly, and accurately. FortiGuard IPS signature clustering empowers security teams to proactively protect their networks, applications, and assets from a multitude of cyberthreats, making it an integral component of any comprehensive cybersecurity strategy.

FORTINET

www.fortinet.com

August 30, 2023 3:07 PM

2312453-0-0-EN