Check Point
SOFTWARE TECHNOLOGIES LTD.

WE SECURE THE FUTURE

Threat Prevention Meta Data

Severity, Performance, Confidence

This document defines how severity, performance and confidence levels are assigned to new protections across various threat prevention blades.

Severity:

IPS

- Low:
  - Vulnerability may lead to information disclosure
  - Vulnerability effect can be easily contained or mitigated
  - Vulnerability exists only in customized configurations of the product
  - Exploit code and vulnerability details are not widely available
  - The vulnerability is already patched when the protection is released
  - There is no apparent way to create an effective exploit
  - The vulnerable software is only moderately deployed
- Medium:
  - Vulnerability which may lead to denial of service
  - Vulnerability exists in general availability release of the product
  - Vulnerability exists in the default configuration of the product
  - The vulnerable software is partially deployed in some enterprises
- High:
  - Vulnerability may lead to non-privileged remote code execution
  - Vulnerability may affect important company assets
  - Vulnerability can be easily exploited
  - The vulnerable software is significantly deployed in corporate environments
- Critical:
  - Vulnerability may lead to remote code execution or administrative level compromise and may affect network infrastructure
  - The vulnerable software is from a major enterprise vendor
  - An exploit for the vulnerability exists in the wild
  - The vulnerability is unpatched at the time the protection is released
  - The vulnerable application or protocol is very common in corporate environments

In addition, a protection severity level can be raised to fit one or more of the following parameters:

- Severity of the exploit according to its CVSS score
- Severity rating of the vulnerability according to the vendor
- Severity rating of the vulnerability according to the entity discovered it

AV/AB

Severity is currently only set to distinguish between adware and malware while adware is assigned with low severity and malware with medium/high severity.

Performance:

IPS

- Very Low (not relevant to AB)
  - All protections which do not cause any performance degradation.
  - New protections are not added to this category without performance tests.
- Low:
  - All simple signatures over any protocol which have very unique traffic patterns.
- Medium:
  - ALL HTTP Client protections which use complex detection logic.
  - All protocol parsers which perform protocol anomaly over PSL.
  - All signatures executed on HTTP responses.
- High:
  - Protections which are executed on all ports.
  - Performs extremely heavy and complex detection logic. For example, decoding of RC4 encryption.
- Critical:
  - Requires deep inspection of a significant portion of the traffic

The performance impact is derived from the complexity of the protection:

The resources the protection uses for inspection.
The amount of traffic inspected due to the nature of the traffic blend (for example: HTTP - lots of traffic, Telnet - little traffic).

Confidence:

Confidence levels are the same across all threat prevention blades:

- Low – Protections which can produce false positives events in high probability.
- Medium – Protections which product false positives events in low probability.
- High – Protections which are reliable in detecting attacks and do not produce any false positives.

