How Risk Rating is Calculated in IOS IPS

Starting in Cisco IOS® Software Release 12.4(11)T, the Cisco IOS Intrusion Prevention System (IPS) feature supports 5.x signature-format-based signatures. It also supports the unique Cisco Risk-Rating-based signature event action processor. Risk ratings are assigned to alerts generated from IPS sensors. The intent of this risk rating is to provide the user with an indication of the relative risk of the traffic or offending host continuing to access the user's network. This rating can be used to provide a means for developing risk-oriented event action policies for Cisco IOS IPS.

The risk rating is realized as an integer value in the range from 0 to 100. The higher the value, the greater the security risk of the trigger event for the associated alert. The risk rating is a calculated number that has three primary components: Alert Severity Rating (ASR), Signature Fidelity Rating (SFR), and Target Value Rating (TVR).

The risk rating is calculated using the following formula:

$$RR = \frac{Fidelity * Severity * Target\text{-}value\text{-}Rating}{100 * 100}$$

The Risk Rating value is rounded to 100 if the calculated value is greater than 100.

Signature Fidelity Rating (SFR)

The SFR is a user-modifiable weighted value that characterizes the fidelity of the signature that has detected the suspect activity. It represents a relative measure of the accuracy of the signature. It has a value of 0 to 100 set by Cisco by default. Under normal circumstances, the user will not change this value.

Several factors affect the fidelity of a signature. First, many vulnerabilities are only relevant for a particular OS, service, application, or even patch level. Without this information, particularly in the classic intrusion detection system (IDS) mode, the sensor may identify attempts that will ultimately fail as actual attacks, leading to wasted effort on the part of the security administrator investigating the alleged attack. Another issue that can cloud the fidelity of a signature is a legitimate application that produces traffic that mimics the behavior of an exploitation of network vulnerability. The signature developer takes these factors into consideration when assigning the SFR for a particular signature.

Alert Severity Rating (ASR)

It has a value of one of the following: 25 (Information), 50 (Low), 75 (Medium), or 100 (High).

The ASR is a user-modifiable weighted value that characterizes the damage potential of the suspect traffic. It is presented to the user in familiar, descriptive text tags: informational, low, medium, and high. Under normal circumstances, the user will not change this value.

- An informational alert is based on commonly seen network traffic and has no particular security relevance when seen on most networks. It may be a violation of a policy on some networks, but it generally poses no immediate threat to network security. Information alert has a value of 25.
- A low alert is also based on relatively benign network traffic, but is somewhat unusual on most networks. Also categorized as low would be overt scans, such as those commonly seen by network management devices. Although this type of scan could be a precursor to an attack, it is uncommon for an overt scan to be used for this purpose. Low alert has a value of 50.
- A medium alert is based on traffic that generally should not be seen on the network. It is usually assigned to midlevel reconnaissance traffic, denial of service (DoS) attacks on self-healing services, and remote access of unexpected information or programs. This type of behavior warrants investigation or preventive actions, sometimes requiring policy decisions from the user. Medium alert has a value of 75.
- A high alert is based on traffic that is indicative of an active attack or an obvious precursor to an attack. This traffic should never be seen in a normal network. This rating is reserved for attacks that could result in serious compromise of the target, or for specific network traffic that is only seen in covert reconnaissance traffic. High alert has a value of 100.

Target Value Rating (TVR)

TVR is a user-defined value that represents the user's perceived value of the target host. This allows the user to increase the risk of an event associated with a critical system and to de-emphasize the risk of an event on a low-value target. It has a value of one of the following: 75 (Low Asset Value), 100 (Medium Asset Value), 150 (High Asset Value), and 200 (Mission-Critical Asset Value). It would not be unusual for a user to raise or lower the TVR of assets to increase the visibility of alerts fired on critical assets, or to decrease the visibility of alerts fired on none critical assets. The default value of TVR is 100—Medium Asset Value.

In closing, risk rating provides the user with valuable insight into the overall risk of an event. This allows the user to develop policies for the prevention of network attacks or to better characterize events for prioritization of further investigation. Risk rating in conjunction with event action overrides makes it very easy for customers to configure Cisco IOS IPS to take action on alerts that exceed a certain risk rating threshold. For example, in most cases, a customer may find that a risk rating of 90 or greater represents a substantial threat on their network. Because all alerts use the same criteria to calculate risk rating, the customer can configure event action override to drop any packets that generate a risk rating of 90 or greater. Subsequently, a risk rating of 50 or less may be of no interest to a customer, so they can use event action override to ignore alerts with ease and lower risk rating calculations.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-400009-00 3/07

