Cumulative SEU Features and Resolved Issues

Last Updated: October 1, 2015
Compatible with Version 4.9.x or 4.10.x of the Sourcefire 3D System

Most SEUs provide new and updated rules and, on occasion, can include new rule categories, new or revised system variables, and revised default settings for intrusion policy features. Additionally, SEUs sometimes provide new features and functionality and resolve issues with existing capabilities. Typically, when an SEU provides new features and functionality and resolves issues with existing capabilities, the SEU includes a new detection engine.

This document describes the new features and functionality and resolved issues in recent SEUs. It does not include the many SEUs that did not provide new features and functionality or resolve issues with existing capabilities. Because SEUs are cumulative, you should be aware of feature updates and issues resolved in any SEU whose number falls between the last SEU you imported and the SEU you plan to import.

This document also provides instructions for importing SEUs on Version 4.9.x and 4.10.x systems, and information for contacting Support.

See the following sections for more information:

Cisco Systems, Inc.
www.cisco.com

Recent SEUs

The following table lists recent SEUs that have provided new features and functionality, resolved issues, or both. The following sections describe the new features and functionality and the issues resolved in these SEUs.

Table 1 Recent SEUs

Release	Detection Engine	Release Date
SEU-1360	Snort® 2.9.7.6	October 1, 2015
SEU-1325	Snort 2.9.7.5	July 22, 2015
SEU-1298	Snort 2.9.7.3	May 19, 2015
SEU-1261	Snort 2.9.7.2	March 3, 2015
SEU-1199	n/a	November 4, 2014
SEU-1194	Snort 2.9.7	October 23, 2014
SEU-1170	Snort 2.9.6.3	September 16, 2014
SEU-1142	Snort 2.9.6.2	July 15, 2014
SEU-1092	Snort 2.9.6.1	April 23, 2014
SEU-1034	Snort 2.9.6	January 22, 2014
SEU-1003	Snort 2.9.5.6	November 18, 2013
SEU-960	Snort 2.9.5.5	September 12, 2013
SEU-937	Snort 2.9.5.4	August 1, 2013
SEU-937	Snort 2.9.5.3	July 24, 2013
SEU-929	Snort 2.9.5.2	July 18, 2013
SEU-915	Snort 2.9.5.1	June 27, 2013
n/a	Snort 2.9.5	June 25, 2013
SEU-863	Snort 2.9.4.6	April 18, 2013
SEU-850	Snort 2.9.4.5	April 1, 2013
SEU-823	Snort 2.9.4.4	February 25, 2013
n/a	Snort 2.9.4.3	February 4, 2013
SEU-786	Snort 2.9.4.2, patch 1	January 24, 2013
SEU-770	Snort 2.9.4.2	December 20, 2012
SEU-766	Snort 2.9.4.1	December 17, 2012
SEU-755	Snort 2.9.4	December 3, 2012
SEU-678	Snort 2.9.3.1	August 8, 2012
SEU-667	Snort 2.9.3	July 17, 2012
SEU-601	Snort 2.9.2.2	March 27, 2012
SEU-583	Snort 2.9.2.1, patch 1	February 23, 2012
SEU-567	Snort 2.9.2.1	January 19, 2012
SEU-552	Snort 2.9.2	December 12, 2011

Table 1 Recent SEUs

Release	Detection Engine	Release Date
SEU-512	Snort 2.9.1.2	October 18th, 2011
SEU-508	Snort 2.9.1.1	October 6, 2011
SEU-489	Snort 2.9.1	August 23, 2011
SEU-438	Snort 2.9.0.5	April 6, 2011

SEU-1360

This section describes the issues resolved in the SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

- Resolved an issue where, if you enabled **Extract Original Client IP Address** and the system detected traffic with multiple HTTP transactions, some with or without XFF data, the system displayed incorrect **Original Client IP** addresses in the Intrusion Events table. (CSCut18532)
- Resolved an issue where configuring an intrusion rule with a **Min TTL** value and a generator ID (GID) of `116` and signature IDs (SID) of `270` or `428`, the system incorrectly dropped the traffic that was below the intrusion rule's **Min TTL** value instead of allowing the traffic to pass. (CSCuu17924)
- Resolved an issue where, if you created a cluster of devices in a high availability configuration and enabled state sharing, the system did not terminate the state sharing session on the secondary device and incorrectly generated `WARNING: Attempt to delete a TCP Session when no valid runtime configuration` messages. (CSCuu97559)

SEU-1325

This section describes the new functionality and the issues resolved in this SEU.

New Features and Functionality

- Snort now ignores several global configuration settings in custom policies. (CSCus61592)

Resolved Issue

- Enhanced Snort detection, processing capabilities, and memory performance when processing asynchronous traffic. (CSCus67155)
- Resolved an issue where Snort generated incorrect alerts or missed alerts for certain email attachments. (CSCus93469)
- Resolved an issue where the system did not generate alerts for rate based attacks. (CSCze95718)

SEU-1298

This section describes the new features and functionality and the issue resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Improved accuracy of detection when dealing with SIP traffic.
- Improved the stability of stream tcp normalization.
- Improved detection coverage in certain cases when stream reassembly is not enabled for a given set of TCP ports or services.
- Resolved an issue where protected_content evaluation did not work when used in correlation to other options within an intrusion rule.

SEU-1261

This section describes the new features and functionality and the issue resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Resolved an issue where the Inline Normalization preprocessor incorrectly resized packets when the **Trim Data to Window** option was enabled.

SEU-1199

This section describes the new features and functionality and the issue resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issue is resolved in this SEU:

- Resolved an issue where applying a VLAN- or network-filtered intrusion policy failed after updating to SEU 1194 or SEU 1195. (CSCur39948)

SEU-1194

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where the system generated a false positive for the SSH preprocessor rule 128:1. (135567)
- Resolved an issue where a custom intrusion rule with a TCP protocol condition generated events in UDP traffic instead of TCP traffic. (136843)
- Resolved an issue where the Modbus preprocessor failed to generate events after the system missed or dropped a packet. (142450).
- Resolved an issue where, if you configured global thresholding using the **Source** tracking method, global thresholding ran using the **Destination** tracking method. (142940)

SEU-1170

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Improved the stability of the DCE/RPC preprocessor. (142199)
- Improved event processing for Modbus/TCP traffic. (142670)

SEU-1142

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issue is resolved in this SEU:

- Improved the stability of Snort when a nightly intrusion event performance statistics rotation occurred at the same time as an intrusion policy apply. (139958)

SEU-1092

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where, in rare cases, Snort stopped processing packets if any of your intrusion rules contained the sensitive data rule classification. (132600)
- Resolved an issue where the system generated an abnormally high count for the **Total Packets Received** Snort real-time statistic. (134036)
- Resolved an issue where the system did not prevent you from reapplying any of your intrusion policies (individually or part of an access control policy reapply) a total of 4096 or more times on a single managed device. (134231)
- Resolved an issue where the system included and displayed rules 116:460 and 116:461 in both the deleted and decoder rule set categories. (135927)
- Security Issue Eliminated a cross-site scripting (XSS) vulnerability (CVE-2014-2012) in the intrusion rule editor pages that could allow an attacker to access and disclose information, imitate user actions and requests, or execute arbitrary JavaScript. Special thanks to Liad Mizrachi Check Point Security Research Team for reporting this issue. (136537)

SEU-1034

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU contains the following new features and functionality:

- You can now use -1 as a minimum value in icode ICMP code range checks. Selecting -1 as the minimum value allows you to include the ICMP code 0 in the range. (124212)
- Added a new SMTP preprocessor alert to detect attacks against Cyrus SASL authentication. (129695, 129696)
- Added several new Snort decoder rules to identify packets containing malformed authentication headers. (132307)

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where lengthy PID filenames from Snort caused the system to generate extraneous health alerts. (123454)
- The system now generates an error message when you attempt to install an intrusion rule update while the system is already running an update of the Sourcefire 3D System. (124290)
- Resolved an issue where the system incompletely terminated failed intrusion rule updates. (125368)
- Resolved an issue where the system generated false positive alerts on the SMTP preprocessor rules 124:1, 124:3, or 124:10. (125449)
- Improved the performance of sensitive data analysis. (125588, 126167)
- Resolved an issue where the system generated false positive alerts in reassembly traffic if you enabled any of the auto-detect DCE/RPC preprocessor options. (125737)
- Resolved an issue where the system generated events on intrusion rule 135:2 for incomplete (SYN-only) connections when you enabled the TCP stream preprocessor option **Require TCP 3-Way Handshake** and you configured the rate-based attack prevention preprocessor to limit excessive simultaneous connections. (127803)
- Resolved an issue where the system generated false positive alerts on intrusion rule 1:24490. (128304)

- Resolved an issue where disabling the **Quoted-Printable Decoding Depth** advanced option in your intrusion policy did not prevent the system from generating events on intrusion rule 124:11. (132538)

SEU-1003

This section describes the new features and functionality and the issue resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Improved the stability of the `byte_extract` keyword and the HTTP inspect preprocessor. (129329, 129843, 130005)

SEU-960

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where, in some cases, the system generated false positive alerts on the SMTP preprocessor rules 124:1 and 124:3. (124688)
- Resolved an issue where the SIP preprocessor generated false positive alerts on packets before packet reassembly. (125808)
- Resolved an issue where, if you created an intrusion policy based on the Security Over Connectivity default intrusion policy with the Latency-Based Rule Handling preprocessor enabled, the system did not populate any of the preprocessor's default values. (126240)
- Improved performance statistics logging to more accurately reflect packet counts per time interval. (126437)

SEU-937

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Resolved an issue where intrusion policies did not apply properly after installing an SEU on a Version 4.10.x Defense Center managing a Version 4.9.x sensor. (126086)

SEU-932

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Resolved an issue where, in certain circumstances, Snort repeatedly restarted if rule 3:20825 was enabled in an intrusion policy, generating health alerts. (126089)

SEU-929

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where, when you saved an intrusion rule with a content keyword containing a search string ending in a colon (:), the system added a backslash (\) to the string. (119707)
- Resolved an issue where, in certain circumstances, the intrusion policy comparison view did not work as intended if the base policy for an intrusion policy was not configured to update when installing a new SEU. (123739)
- Added rule documentation for GID 140 rules. (124111)

SEU-915

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU contains the following new features and functionality:

- Added, modified, and removed numerous preprocessor rules. (102633, 104588, 111941, 113970, 118178, 118500, 118553, 122038)
- Improved the content keyword. If a negative distance value associated with the content keyword sets the starting point for the content search before the beginning of the data, the search will start at the beginning of the data. Using the content keyword to analyze a URI now alerts on every match, in addition to the first, within the URI. (109059, 118112)
- Added a new troubleshooting option to the Performance Statistics configuration. Enabling the **Summary** option now logs statistics only when a detection engine is shut down or restarted. (110470)

- Improved the packet decoder to support decoding ERSPAN type 2 and ERSPAN type 3 traffic. (113675)
- Improved the HTTP inspect preprocessor to exclude proxy information when inspecting normalized URIs. (118025)
- Resolved an issue where, after an automatic intrusion policy apply, an invalid local rule prevented Snort from starting correctly. (124935)

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where searching for intrusion events using negated IPv6 addresses resulted in incorrect search results. (101015)
- Resolved an issue where the table view of intrusion events did not properly display XFF data. (102655, 110873)
- Resolved an issue with the intrusion policy comparison not properly showing all differences between intrusion policies after an SEU import. (107911)
- Resolved an issue where rules did not generate events if they defined SIP methods in the `sip_method` keyword that were not already defined in the SIP preprocessor. (110532)
- Resolved an issue where reports generated graphs and charts without labels for portscan events. (110828)
- Improved the TCP stream preprocessor to reduce false positives related to data overlap anomalies in TCP segments. (111871)
- Resolved an issue where, in certain cases, intrusion events generated from reassembled traffic did not contain packet data. (112519)
- Resolved an issue where logged packet data did not contain XFF data. (113369)
- Resolved an issue where the detection engine restarted during intrusion policy apply due to detected SMTP preprocessor changes, even if there were no changes to the SMTP preprocessor. (116830)
- Resolved an issue that prevented you from suppressing a GID 134 rule. (117593)
- Resolved an issue where the HTTP inspect preprocessor did not properly inspect pipelined requests. (118713)
- Resolved an issue where the HTTP inspect preprocessor swapped the source and destination IP addresses when detecting packets containing the same source and destination ports. (119009)
- Resolved an issue where you could not add targets to an intrusion policy on a standalone sensor. (119055)
- Improved the IP defragmentation preprocessor to avoid a possible exploit using packet fragments. (119531)
- Resolved an issue where intrusion rules using the `file_data` keyword did not drop traffic if **Drop when Inline** was disabled in the default intrusion policy. (120156)
- Resolved an issue where the TCP stream preprocessor did not correctly identify the server in HTTP traffic detected midstream while adaptive profiles were enabled. (120170)
- Improved the TCP stream preprocessor to reduce false positives when detecting traffic midstream while adaptive profiles were enabled. (120171, 122391)
- Improved the packet decoder to better decode Teredo traffic. (120292)

- Resolved an issue where if you created a custom intrusion policy based on a default intrusion policy, then created another custom intrusion policy based on that first policy, the intrusion policy editor was inaccessible. (120970)
- Resolved an issue where, in rare cases, sensors did not correctly log intrusion events. (122130)
- Resolved an issue where users were not prompted to enable the TCP stream preprocessor when saving an intrusion policy with the rate-based attack prevention preprocessor enabled and the TCP stream preprocessor disabled. (122811)
- Resolved an issue where, in rare cases, rules that triggered on pruned sessions applied the rule action to current sessions. (122990)
- Resolved an issue where, in some cases, analyzing data connections generated a health alert related to sensor memory. (124603)

SEU-863

This section describes the new features and functionality and the issues resolved in this SEU.

New Feature and Functionality

This SEU contains the following new feature and functionality:

- Improved the FTP and telnet preprocessor to better parse FTP command parameter validation statements, reducing false positives. (119869)

Resolved Issue

The following issue is resolved in this SEU:

- Resolved an issue where, in rare cases, saving an intrusion policy with empty fields in the advanced settings made the intrusion policy editor inaccessible for that policy. (119928)

SEU-850

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where, in certain cases, packet data for intrusion events logged incorrectly. (118181)
- Improved the HTTP inspect preprocessor to better analyze URIs containing proxy information. (118487)

SEU-823

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue where events generated due to a Security Intelligence-blacklisted IP address were counted as intrusion events in performance statistics and the health monitor. (115855)
- Resolved an issue where, in rare cases, the TCP stream preprocessor and the inline normalization preprocessor would improperly block SYN-ACK packets from servers. (117745)

SEU-786

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Resolved an issue where applying an intrusion policy restarted Snort, generating a health alert and resulting in traffic not being inspected during the policy apply. (116068)

SEU-770

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Improved the stability of intrusion policies applied to specific targets. (114177, 114319)

SEU-766

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Resolved an issue that prevented the detection engine from operating correctly for certain configurations. (113851)

SEU-755

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Modified the Performance Monitor to alert on and log information on fast-pathed traffic. (97091)
- Resolved an issue where, in some cases, after you install a new SEU on an appliance, the Modified By column on that appliance's Intrusion Policy page shows an incorrect user as the user who applied the update. (100468)
- Resolved an issue where creating a custom intrusion policy using another custom intrusion policy as your base policy, then continuing to create custom policies using the newly created policy as the base policy, would eventually prevent the policy edit page from loading. You can now create a maximum of five chained custom policies in this manner. (104367)
- Resolved an issue with intrusion policy advanced configuration settings that prevented the intrusion policy comparison report from loading. (104852, 104853)
- Modified the intrusion policy rules filter to exclude invalid rules that otherwise match the filter criteria. (105136)
- Improved the TCP stream preprocessor to alert on TCP sessions lacking a three-way handshake. (105352)
- Resolved an issue where, in some cases, automatic intrusion policy reapply after an SEU import would fail if a policy was applied to more than one device. (106210)
- Improved the SSL preprocessor to better identify and process encrypted traffic and related intrusion rules. (106296)
- Improved the inline normalization preprocessor to allow retransmitted SYN packets and reduce false positive alerts. (106316)
- Resolved an issue where email alerting for preprocessor and sensitive data rules could not be disabled without entirely disabling email alerting. (106901)
- Modified the TCP stream preprocessor to reduce false positives. (107614)
- Improved cross-site scripting security. (107669)
- Resolved an issue where intrusion policy layers displayed incorrect rule state colors. (108332)
- Resolved an issue that prevented users from creating intrusion policies on Master Defense Centers. (109053)
- Added rules 119:31 and 119:32 for the HTTP inspect preprocessor. (109063)

SEU-678

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issue

The following issue is resolved in this SEU:

- Improved handling of active responses for certain types of TCP traffic. (106012)

SEU-667

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU contains the following new features and functionality:

- A new global option (**Auto-Detect Policy on SMB Session**) for the DCE/RPC preprocessor detects the Windows or Samba version that is identified in SMB Session Setup AndX requests and responses. This overrides the configured version for that session only when the detected version is different.
- The `flowbits` keyword in the intrusion rule editor now allows AND and OR logic when setting and evaluating states. You can set, unset, or toggle multiple specified states at once. You can also evaluate whether any or all states are set or unset in a group, whether multiple specified states are all set or unset on a packet, and whether any specified state is set or unset on a packet.
- Groups are no longer mutually exclusive with respect to states. A state can belong to multiple `flowbits` groups. You can now set a state in a group without unsetting all other states in that group.

Resolved Issues

- The following issues are resolved in this SEU:
- Removed support for the deprecated xlink2state preprocessor. The xlink2state preprocessor has been superseded by the SMTP preprocessor since the first SEU release. If you configured the xlink2state preprocessor in the user.conf configuration file, you must remove that configuration. (97380)
- Added thresholding, suppression, and SNMP alerting for rate-based attack events. (99214)
- Improved the accuracy of and reduced false positives generated by the SIP, DCE/RPC, and Sensitive Data preprocessors. (100334, 101164, 103894)
- Added support to exclude an IP address from a CIDR block in the intrusion rule editor. (100420)
- Improved MIME email attachment inspection and alerting for the IMAP, POP, and SMTP preprocessors. (100509, 100872)
- Improved the accuracy of non-port bound IPS rules when a service is identified. (101207)
- Improved the accuracy of HTTP processing for HTTP rules. (102515)
- Improved the stability of the Performance Monitor. (103219)
- Improved the stability of Snort sessions. (103587)
- Resolved an issue where enabling adaptive profiling would result in unresolved variables. (103666)
- Resolved an issue with inconsistent preprocessor initialization order on Snort restart versus Snort reload. (104100)
- Resolved an issue where system variables would not be correctly applied to sensors when applying an intrusion policy from the Master Defense Center. (104206)
- Resolved an issue where, in rare cases, logging MIME attachments for the SMTP preprocessor could restart the detection engine. (104861)

- Improved performance for inline deployments when transferring files larger than 2 GB. (104904)

SEU-601

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue with SNMP alerts configured to contain string value IP addresses containing binary value IP addresses. (97490)
- Modified the DCE/RPC preprocessor to generate fewer false positive alerts. (98233)
- Modified the SIP preprocessor to generate fewer false positive alerts. (98787)
- Removed individual rule actions for rules with GID 135. (99213)
- Resolved an issue which prevented you from saving as a new rule any rule that contains documentation references. (99305)
- Resolved an issue where SEU imports did not apply the proper permissions to created directories. (99455)
- Resolved an issue with the Intrusion Policy page displaying intrusion policies with large numbers of enabled rules. (100408)

SEU-583

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

The Resolved Issues section for this SEU includes new features and functionality that resulted from resolving the issues described in that section.

Resolved Issues

The following issues are resolved in this SEU:

- Added a new `reference` keyword argument (**msb**) to simplify linking intrusion rule references to specific Microsoft security bulletins. (94869)
- Added a new option (**Normalize TCP Excess Payload**) for the Inline Normalization preprocessor to improve normalization of TCP traffic. (96288)
- Added a new `reference` keyword argument (**secure-url**) to allow intrusion rule references to include HTTPS URLs. (96379)
- You can now filter rules in an intrusion policy to display new or changed rules imported in an SEU. (96899)
- Resolved an issue where filtering rules in the intrusion rule editor would yield unexpected results. (97063)

- Added a new Detection Settings configuration page, accessible from the intrusion policy Advanced Settings page, which allows you to correctly process traffic for your deployment by ignoring the VLAN header in traffic traveling in different directions for the same connection or flow. (97114)
- Improved intrusion policy validation. (97135)

SEU-567

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- You can now configure the HTTP Inspect preprocessor to alert on unknown HTTP method types. (94748, 97843)
- Resolved a latency issue with the DCE/RPC preprocessor that occurred when automatic detection of TCP ports greater than 1024 was enabled. (96512)
- You can now configure the HTTP Inspect preprocessor to alert on version 0.9 of the HTTP protocol. (96732, 97924)
- Resolved an issue with the GTP preprocessor where an invalid GTP version 1 header length caused the system to stop alerting. (97765)
- Resolved an issue where an out-of-order TCP acknowledgement could interrupt detection. (97830, 98121)

SEU-552

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU contains the following new features and functionality:

- A new GTP preprocessor detects anomalies in version 0, 1, and 2 GTP traffic and forwards command channel signaling messages for these versions to the rules engine for inspection. You can use several new GTP rule keywords to inspect GTP command channel traffic for exploits.
- New Modbus and DNP3 preprocessors detect anomalies in Modbus and DNP3 SCADA traffic and forward data to the rules engine for inspection. You can use several new Modbus and DNP3 keywords to inspect Modbus and DNP3 protocol fields for exploits.
- A new HTTP Inspect preprocessor option detects and normalizes Javascript data in HTTP responses. You can use the `file_data` keyword to point intrusion rules to the normalized Javascript data.

Resolved Issues

The following issues are resolved in SEU 552:

- Intrusion rule keywords that follow the `dce_stub_data` keyword in a rule now continue to refer to the stub data unless a subsequent `pkt_data` or `file_data` keyword changes the reference to the payload data. This includes subsequent relevant and absolute positioning keywords. (89646)

- Resolved an issue where using the maximum memory allocated to the DCE/RPC preprocessor could result in false positives. (90643)
- Resolved an issue where, in rare cases, packets matching a drop rule might not be inspected in heavy traffic. (90870)
- Resolved an issue where only one `content` keyword in a rule could combine the **HTTP URI**, **Distance**, and **Within** arguments. (91671)
- Resolved an issue where an intrusion policy did not use system variables created on a Master Defense Center. (92387)
- Resolved an issue that prevented intrusion policies from synchronizing when you modified the intrusion policy on the secondary Defense Center in a high availability pair. (92822)
- Resolved an issue where the system did not report the correct original client IP address when the address changed during a long session in HTTP proxy traffic. (92995)
- Improved event logging performance. (94114)
- Resolved an issue where rolling back an SEU to a previous version deleted locally created intrusion rules that were created after the previous SEU and renumbered older ones. (94813)
- Resolved an issue where unknown host attributes resulted in an error message when adaptive profiles were enabled. (95032)
- Improved the detection capabilities of the Sun RPC, DCE/RPC, HTTP Inspect, and FTP/Telnet preprocessors. (89384, 90643, 92256, 95392)

SEU-512

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issue is resolved in this SEU:

- In rare cases, inline traffic could be disrupted when a persistent HTTP 1.1 session with a UTF-32 encoded response is followed by a UTF-16 encoded response in the same session. (94728)

SEU-508

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Improved the detection capabilities of the HTTP and DCE/RPC preprocessors with more vigorous TCP reassembly methods. (91305)
- Reduced false positives that sometimes occurred when using the `urilen` rule keyword. (91849)

- Improved system performance and detection. (91894, 92062, 92255)

SEU-489

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

When you import the SEU on an appliance that is using Version 4.9.x or later:

- A new session initiation protocol (SIP) preprocessor decodes SIP traffic, detects anomalous behavior, and passes the traffic to the rules engine for inspection. Four new SIP keywords allow you to use intrusion rules to inspect SIP session traffic for exploits.
- New IMAP and POP preprocessors, and updates to the SMTP preprocessor, decode email attachments in IMAP4, POP3 and SMTP traffic, respectively, detect anomalies, and send decoded attachments to the rules engine for inspection. Updates to the `file_data` keyword allow you to use intrusion rules to inspect the decoded email attachments.
- The `file_data` keyword now points to specific payload types based on the type of traffic detected. The `file_data` MIME argument is deprecated and, when encountered in intrusion rules, is ignored with no loss in functionality. For appliances other than IPSx, which has no rule editor, editing and saving a rule removes any instance in the rule of the MIME argument.
- A new SMTP preprocessor **Base64 Decoding Depth** option replaces the **Enable MIME Decoding** and **Maximum MIME Decoding Depth** options. If **Enable MIME Decoding** is enabled in an intrusion policy when you import the SEU, the system enables the new **Base64 Decoding Depth** option on a layer-by-layer basis by setting the new option to the value that was set in each layer for **Maximum MIME Decoding Depth**.
- A new `pkt_data` intrusion rule keyword points to the beginning of a normalized SMTP, FTP, or telnet packet payload; for other detected traffic, `pkt_data` points to the beginning of the raw TCP or UDP payload.
- Three new HTTP Inspect preprocessor configuration options (**Maximum Number of Spaces**, **Small Chunk Size**, and **Consecutive Small Chunks**) can generate events on anomalous packets.

In addition to the above features, when you import the SEU on an appliance other than IPSx that is using Version 4.10.1 or later:

- You can view the IPv6 source address and destination address for the packet that triggers an intrusion event.
- You can view, if present, the host name and host URI associated with an HTTP request packet that triggers an intrusion event. Two new HTTP configuration options (**Log Hostname** and **Log URI**) enable display of the data. Note that 3D500 and 3D1000 sensors do not provide host name and URI data.
- You can view email attachment file names and the email sender and recipient addresses for packets that trigger intrusion events. Three new SMTP preprocessor configuration options (**Log MIME Attachment Names**, **Log To Addresses**, and **Log From Addresses**) enable display of the data.
- Two new SMTP configuration options (**Log Headers** and **Header Log Depth**) allow you to extract email headers for inspection by the rules engine.

Resolved Issues

The following issues are resolved in this SEU:

- Improved the performance of several scan detection rules. (80944, 80945, 80959)
- Limited the number of layers in an intrusion policy to 200. (81916.)

- Resolved an issue with the HTTP Inspect preprocessor where parsing of HTTP methods could result in false positives. (82256)
- Resolved an issue with the packet decoder where certain UDP packets could trigger false positives when Teredo tunneling on non-standard ports was enabled. (81698, 82477)
- Resolved an issue where packets tagged by the system could cause false positives after the global rule threshold was reached. (85994)
- The audit log now attributes changes to the admin user, not the user who last modified an intrusion policy, when an SEU makes changes to the policy. (86811)
- Resolved a synchronization issue that could occur when peers in a high availability pair had different SEUs installed. (88303)
- Resolved an issue that resulted in false negatives in PPPoE traffic. (88729)
- Prevented a circular dependency by prohibiting shared layers in a custom base policy. (89459)

SEU-438

This section describes the new features and functionality and the issues resolved in this SEU.

New Features and Functionality

This SEU does not include any new or updated features.

Resolved Issues

The following issues are resolved in this SEU:

- Resolved an issue that prevented the web interface from displaying some types of performance data. (83414)
- Improved the stability of Snort as it inspects specific types of traffic. (84551, 85215, 84587)
- Resolved an issue where the packet decoder incorrectly dropped fragmented ICMPv6 packets. (85010)
- Resolved an issue with the `cvs` rule keyword that could cause false positives. (85093)
- Resolved an issue where an active response triggered by a packet tagged for VLAN traffic resulted in an incorrectly encoded RST packet. (85316)
- Resolved an issue where reapplying an intrusion policy after importing an SEU did not correctly apply all intrusion policy settings when the **Inspect Traffic During Policy Apply** detection engine option was enabled. (85547)
- Resolved an issue where packets dropped by the inline normalization preprocessor did not trigger events. (85549)
- Modified the default behavior of the inline normalization preprocessor so that when you enable the **Normalize IPv4** option, the default normalizations no longer include truncating packets with excess payload or clearing the Differentiated Services (DS) field, formerly known as the Type of Services (TOS) field. Contact Support for instructions on adding these normalizations. (85551, 85552)
- Improved performance of the inline normalization preprocessor. (85553)
- Resolved an issue where the inline normalization preprocessor might incorrectly set TCP Time Stamp option bytes to No Operation (TCP Option 1). (85951)

Importing the SEU

As new vulnerabilities become known, the Vulnerability Research Team (VRT) releases Security Enhancement Updates (SEUs).

An SEU contains new and updated standard text rules and shared object rules that you can use to detect potential attacks against your network and its assets. An SEU may also provide an updated version of Snort, as well as features such as new preprocessors and decoders. Importing an SEU installs the changes in the SEU on the appliance where you import it. When you apply a policy that implements new or modified SEU components supported by the version of system software running on a managed 3D Sensor, and the SEU has not been installed on the sensor, the system pushes the necessary SEU components to the sensor.

Note SEUs may contain new binaries. Make sure your process for downloading and installing SEUs complies with your security policies. In addition, SEUs may be quite large, so make sure you import SEUs during periods of low network use.

See the following sections for more information:

- Importing SEUs on Version 4.9.x or 4.10.x of the Sourcefire 3D System, page 19
- Importing SEUs on Sourcefire IPSx, page 23

Importing SEUs on Version 4.9.x or 4.10.x of the Sourcefire 3D System

The following are important points you should keep in mind when you import an SEU on a Sourcefire 3D System appliance:

- VRT often includes new rules in SEUs, with the rule state set for each default policy. For example, a new rule may be enabled in the Security over Connectivity default policy and disabled in the Connectivity over Security default policy. Sometimes VRT also uses an SEU to change the default state of existing rules.
- SEUs are cumulative, so the newest SEU contains the intrusion rules and new features of all previous SEUs. You cannot import an SEU with a version number lower than the version of the currently installed SEU.
- Optionally, an SEU may add new and updated features to the base policy in intrusion policies you create, including new default feature settings, new rules set to their default rule states, and modified default rule states of existing rules. An SEU adds new rules and other features, and updates default feature settings and rule states, according to whether you choose for your base policy to be updated based on updates in the SEU.
- Importing an SEU discards any unsaved edits to an intrusion policy.
- If your Sourcefire 3D System deployment includes two Defense Centers configured as a high availability pair, you need to import the SEU on only one of the Defense Centers. The second Defense Center receives the SEU as part of the regular synchronization process.
- Optionally, when the import completes, you can automatically reapply intrusion policies owned by the appliance where you import the SEU. Note that an appliance owns policies applied from that appliance. For example, a Defense Center owns a policy that it applies to a detection engine on a managed 3D Sensor, and a standalone 3D Sensor owns a policy that it applies to its own detection engine.

- After importing an SEU, applying an intrusion policy from a Defense Center to a detection engine on a managed sensor does not install the SEU on the sensor. However, applying the policy provides the detection engine with any new rules or other features that you enable in the policy even though the new rules or other features you enable are not accessible from the sensor's web interface.
- You can use the **Reapply All** or **Reapply Intrusion Policies** option on the Detection Engines page (**Operations > Configuration > Detection Engines**) to reapply your intrusion policies. These options can be convenient, for example, if you import an SEU and do not automatically reapply your intrusion policies after the import completes. These options conveniently reapply filtered and non-filtered intrusion policies simultaneously for each detection engine.

See the following sections for more information:

- Using Manual One-Time SEU Imports, page 20 to manually download an SEU from the Sourcefire Support web site to your local machine and then manually install the SEU.
- Using Automatic One-Time SEU Imports, page 21 to use an automated feature on the web interface to search the Sourcefire Support site for new SEUs and upload them.
- Using Recurring SEU Imports, page 22 to use an automated feature on the web interface to download and install SEUs from the Sourcefire Support site and, optionally, set the rules state for new rules and reapply your intrusion policy.

Using Manual One-Time SEU Imports

The following procedure explains how to import a new SEU manually. This procedure is especially useful if your Defense Center or sensor does **not** have Internet access.

To manually import an SEU:

Step 1 From a computer that can access the Internet, access and log into Sourcefire Support (https://support.sourcefire.com/).

Step 2 Click **Downloads**, then click **SEU**.

Step 3 Navigate to the latest SEU.

Step 4 Click the SEU file that you want to download and save it to your computer.

Step 5 Log into your appliance's web interface.

Step 6 Select **Policy & Response > IPS > SEU**.

The SEU page appears.

Step 7 Click **Import SEU**.

The Import SEU page appears.

Tip You can also click **Import Rules** on the Rule Editor page, which you access by selecting **Policy & Response > IPS > Rule Editor**.

Step 8 Optionally, click **Delete All Local Rules** then click **OK** to move all user-defined rules that you have created or imported to the deleted folder.

Step 9 Select **SEU or text rule file to upload and install** and click **Browse** to navigate to and select the SEU file.

Step 10 Optionally, select **Reapply intrusion policies after the SEU import completes** to automatically reapply intrusion policies currently applied from this appliance when the SEU import completes.

Note that you **cannot** apply intrusion policies to stacked sensors running different versions of the Sourcefire 3D System (for example, if an upgrade on one of the sensors fails).

Step 11 Click **Import**.

The SEU is installed and the rules are updated. The system displays the SEU Detail View workflow.

Unless you selected **Reapply intrusion policies after the SEU import completes** in step 10, any rule changes are not implemented until the next time you apply the affected intrusion policies.

Note Contact Support if you receive an error message while installing the SEU.

Using Automatic One-Time SEU Imports

The following procedure explains how to import a new SEU by automatically connecting to the Sourcefire Support site. You can use this procedure **only** if the appliance has Internet access.

To automatically import an SEU:

Step 1 Select **Policy & Response > IPS > SEU**.

The SEU page appears.

Step 2 Click **Import SEU**.

The Import SEU page appears.

Tip You can also click **Import Rules** on the Rule Editor page, which you access by selecting **Policy & Response > IPS > Rule Editor**.

Step 3 Optionally, click **Delete All Local Rules** then click **OK** to move all user-defined rules that you have created or imported to the deleted folder.

Step 4 Select **Download new SEU from the support site**.

Step 5 Optionally, select **Reapply intrusion policies after the SEU import completes** to automatically reapply intrusion policies currently applied from this appliance when the SEU import completes.

Note that you **cannot** apply intrusion policies to stacked sensors running different versions of the Sourcefire 3D System (for example, if an upgrade on one of the sensors fails).

Step 6 Click **Import**.

The SEU is installed and the rules are updated. The system displays the SEU Detail View workflow.

Unless you selected **Reapply intrusion policies after the SEU import completes** in step 5, any rule changes are not implemented until the next time you apply the affected intrusion policies.

Note Contact Support if you receive an error message while installing the SEU.

Using Recurring SEU Imports

You can configure daily, weekly, or monthly SEU imports on the Import SEU page. This feature is conveniently located on the Import SEU page to be near SEU import log information. You can also schedule SEU imports from the Scheduling page.

If your Sourcefire 3D System deployment includes two Defense Centers configured as a high availability pair, you need to import the SEU on only one of the Defense Centers. The second Defense Center receives the SEU as part of the regular synchronization process.

To schedule recurring SEU imports:

Step 1 Select **Policy & Response > IPS > SEU**.

The SEU page appears.

Step 2 Click **Import SEU**.

The Import SEU page appears.

Note You can also click **Import Rules** on the Rule Editor page, which you access by selecting **Policy & Response > IPS > Rule Editor**.

Step 3 Optionally, click **Delete All Local Rules** then click **OK** to move all user-defined rules that you have created or imported to the deleted folder.

Step 4 Select **Enable Recurring SEU Imports**.

The page expands to display options for configuring recurring imports.

Import status messages appear beneath **Recurring SEU Imports**. Recurring imports are enabled when you save your settings.

Note To disable recurring imports, clear the **Enable Recurring SEU Imports** check box and click **Save**.

Step 5 In the **Import Frequency** field, select **Daily**, **Weekly**, or **Monthly** from the drop-down list.

Tip You can select from a recurring task drop-down list either by clicking on your selection or by typing the first letter or number in the selection one or more times and pressing Enter.

Step 6 If you selected **Weekly** in the **Import Frequency** field, use the drop-down list that appears to select the day of the week when you want to import SEUs.

Step 7 If you selected **Monthly** in the **Import Frequency** field, use the drop-down list that appears to select the day of the month when you want to import SEUs.

Step 8 In the **Import Frequency** field, specify the time when you want to start your recurring SEU import.

Step 9 Optionally, select **Reapply intrusion policies after the SEU import completes** to automatically reapply intrusion policies currently applied from this appliance when the SEU import completes.

Note that you cannot apply intrusion policies to stacked sensors running different versions of the Sourcefire 3D System (for example, if an upgrade on one of the sensors fails).

Step 10 Click **Save** to enable recurring SEU imports using your settings.

The status message under **Recurring SEU Imports** changes to indicate that the SEU has not yet run.

The SEU is installed at the scheduled time and the rules are updated. You can log off or use the web interface to perform other tasks before or during the import. When accessed during an import, the SEU Import Log page displays a red status icon. During an import, you can also view messages as they occur in the SEU Detail View.

Note Depending on SEU size and content, several minutes may pass before status messages appear in the SEU Import Log or SEU Detail View.

Unless you selected **Reapply intrusion policies after the SEU import completes** in step 9, any rule changes are not implemented until the next time you apply the affected intrusion policies.

Applicable subtasks in the SEU import occur in the following order: download, install, base policy update, and policy reapply. Once one subtask completes, the next subtask begins. Note that you can apply only policies previously applied by the appliance where the recurring import is configured.

Note Contact Support if you receive an error message while installing the SEU.

Importing SEUs on Sourcefire IPSx

The following are important points you should keep in mind when you import an SEU on a Sourcefire IPSx Defense Center:

- VRT often includes new rules in SEUs, with the rule state set for each default policy. For example, a new rule may be enabled in the Security over Connectivity default policy and disabled in the Connectivity over Security default policy. Sometimes VRT also uses an SEU to change the default state of existing rules.
- SEUs are cumulative, so the newest SEU contains the intrusion rules and new features of all previous SEUs. You cannot import an SEU with a version number lower than the version of the currently installed SEU.
- Optionally, an SEU may add new and updated features to the base policy in intrusion policies you create, including new default feature settings, new rules set to their default rule states, and modified default rule states of existing rules.
- Importing an SEU discards any unsaved edits to an intrusion policy.
- You can use the **Reapply All** or **Reapply Intrusion Policies** option on the Detection Engines page (**Operations > Detection Engines**) to reapply your intrusion policies. These options can be convenient, for example, if you import an SEU and do not automatically reapply your intrusion policies after the import completes. These options conveniently reapply filtered and non-filtered intrusion policies simultaneously for each detection engine.

See the following sections for more information:

- Using Manual One-Time SEU Imports, page 24 to manually download an SEU from the Sourcefire Support web site to your local machine and then manually install the SEU.
- Using Automatic One-Time SEU Imports, page 24 to use an automated feature on the web interface to search the Sourcefire Support site for new SEUs and upload them.

- Using Recurring SEU Imports, page 25 to use an automated feature on the web interface to download and install SEUs from the Sourcefire Support site and, optionally, set the rules state for new rules and reapply your intrusion policy.

Using Manual One-Time SEU Imports

The following procedure explains how to import a new SEU manually. This procedure is especially useful if your Defense Center does not have Internet access.

To manually import an SEU:

Step 1 From a computer that can access the Internet, access and log into Sourcefire Support (https://support.sourcefire.com/).

Step 2 Click **Downloads**, then click **SEU**.

Step 3 Navigate to the latest SEU.

Step 4 Click the SEU file that you want to download and save it to your computer.

Step 5 Log into your appliance's web interface.

Step 6 Select **Policy & Response > SEU/Rule Import**.

The SEU/Rule Import page appears.

Step 7 Click **Import SEU**.

The Import SEU page appears.

Step 8 Optionally, click **Delete All Local Rules** then click **OK** to remove all custom rules that you have imported.

Step 9 Select **SEU or text rule file to upload and install** and click **Browse** to navigate to and select the SEU file.

Step 10 Optionally, select **Reapply intrusion policies after the SEU import completes** to automatically reapply intrusion policies currently applied from this appliance when the SEU import completes.

Step 11 Click **Import**.

The SEU is installed and the rules are updated. The system displays the SEU Details page.

Unless you selected **Reapply intrusion policies after the SEU import completes** in step 10, any rule changes are not implemented until the next time you apply the affected intrusion policies.

Note Contact Support if you receive an error message while installing the SEU.

Using Automatic One-Time SEU Imports

The following procedure explains how to import a new SEU by automatically connecting to the Sourcefire Support site. You can use this procedure only if the appliance has Internet access.

To automatically import an SEU:

Step 1 Select **Policy & Response > SEU/Rule Import**.

The SEU/Rule Import page appears.

Step 2 Click **Import SEU**.

The Import SEU page appears.

Step 3 Optionally, click **Delete All Local Rules** then click **OK** to move all user-defined rules that you have imported to the deleted folder.

Step 4 Select **Download new SEU from the support site**.

Step 5 Optionally, select **Reapply intrusion policies after the SEU import completes** to automatically reapply intrusion policies currently applied from this appliance when the SEU import completes.

Step 6 Click **Import**.

The SEU is installed and the rules are updated. The system displays the SEU Detail View workflow.

Unless you selected **Reapply intrusion policies after the SEU import completes** in step 5, any rule changes are not implemented until the next time you apply the affected intrusion policies.

Note Contact Support if you receive an error message while installing the SEU.

Using Recurring SEU Imports

You can configure daily, weekly, or monthly SEU imports on the Import SEU page. This feature is conveniently located on the Import SEU page to be near SEU import log information. You can also schedule SEU imports from the Scheduling page.

To schedule recurring SEU imports:

Step 1 Select **Policy & Response > SEU/Rule Import**.

The SEU/Rule Import page appears.

Step 2 Click **Import SEU**.

The Import SEU page appears.

Step 3 Optionally, click **Delete All Local Rules** then click **OK** to move all user-defined rules that you have imported to the deleted folder.

Step 4 Select **Enable Recurring SEU Imports**.

The page expands to display options for configuring recurring imports.

Import status messages appear beneath **Recurring SEU Imports**. Recurring imports are enabled when you save your settings.

Tip To disable recurring imports, clear the **Enable Recurring SEU Imports** check box and click **Save**.

Step 5 In the **Import Frequency** field, select **Daily**, **Weekly**, or **Monthly** from the drop-down list.

Tip You can select from a recurring task drop-down list either by clicking on your selection or by typing the first letter or number in the selection one or more times and pressing Enter.

Step 6 If you selected **Weekly** in the **Import Frequency** field, use the drop-down list that appears to select the day of the week when you want to import SEUs.

Step 7 If you selected **Monthly** in the **Import Frequency** field, use the drop-down list that appears to select the day of the month when you want to import SEUs.

Step 8 In the **Import Frequency** field, specify the time when you want to start your recurring SEU import.

Step 9 Optionally, select **Reapply intrusion policies after the SEU import completes** to automatically reapply intrusion policies currently applied from this appliance when the SEU import completes.

Step 10 Click **Save** to enable recurring SEU imports using your settings.

The status message under **Recurring SEU Imports** changes to indicate that the SEU has not yet run.

The SEU is installed at the scheduled time and the rules are updated. You can log off or use the web interface to perform other tasks before or during the import. When accessed during an import, the SEU Import Log page displays a red status icon. During an import, you can also view messages as they occur in the SEU Detail View.

Note Depending on SEU size and content, several minutes may pass before status messages appear in the SEU Import Log or SEU Detail View.

Unless you selected **Reapply intrusion policies after the SEU import completes** in step 9, any rule changes are not implemented until the next time you apply the affected intrusion policies.

Applicable subtasks in the SEU import occur in the following order: download, install, base policy update, and policy reapply. Once one subtask completes, the next subtask begins. Note that you can apply only policies previously applied by the appliance where the recurring import is configured.

Note Contact Support if you receive an error message while installing the SEU.

For Assistance

All new support cases must be opened using the Cisco Technical Assistance Center (TAC) by phone, web or email. To open a TAC case online, you must have a Cisco.com user ID and contract number. If you need assistance opening a case, call the Cisco TAC at 800-553-2447.

- Visit the Cisco Support site at http://support.cisco.com/.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.