Root Cause Analysis

Issue:

Performance and compatibility issues were reported on some enterprise Java applications after applying the June 10, Host IPS security content version (5709).

Cause:

The issues were confirmed to be related to previously added Java sandbox escaping prevention JRE software libraries, (added for signature 6666 in the May 27 security content version (5660) release). This release was subsequently withdrawn on June 1 and replaced with remediation content version (5664), which reverted actual signature content back to the that equal to the May 13 security content release (5626). The subsequent posting of the June 10 security content version (5709), inadvertently included code related to the loading of McAfee content related libraries into the system's Java Runtime Engine (JRE) process.

McAfee's analysis of content version (5709) indicates errant injection code remained, which caused libraries related to “Signature 6666-Java Sandbox Exploit Protection (JSEP)”, (jsbp.dll and jsbp.jar files) to load into the system's Java Runtime Engine (JRE) process.

As such, this loading fault during JRE process initialization could cause performance related issues similar to those reported for signature 6666, in the (5660) content version release, even though signature 6666 had been fully removed from the June content posting. The performance issues could lead to Java application hangs, slowness, or other issues related to loading Java applets.

Additional Information:

Under the current implementation of JSEP protection for the Host IPS product, new JRE related libraries were added to the Host IPS installation folder during the original May 27 security content version (5660) release. These libraries would not have been removed during content remediation. As such, the library files (jsbp.dll and jsbp.jar), remained on systems which previously had content version 5660 installed. By design, the related dlls should only load into memory if supporting code is present in the process injection library within Host IPS content.

Root Cause Analysis

Status Summary:

The issue was quickly corrected upon initial customer reports, and on June 12, McAfee withdrew content version 5709 and replaced with an updated content version 5710, available to customers which immediately resolved the issue. No additional customer reports for FPs related to this event are being received.

A McAfee review indicated the errant injection code for the JRE related libraries was not detected during McAfee formal pre-release software code reviews, nor were any related issues reported during McAfee internal QA and pre-release customer (RTS) testing.

Expected Deliverable for JSEP enabled content protection:

McAfee is currently conducting a full process review and have inserted new process checkpoints to ensure a similar issue does not occur in future Host IPS security content updates. McAfee is withholding re-release estimates for Host IPS Signature 6666, JSEP content, until we finalize solutions for reported issues, and have full confidence to validate JSEP signature functionality prior to release. External customer messaging will sent when further updates related to this functionality are confirmed.

Event Timeline:

22:00 GMT on 10-Jun-2014: HIPS Content 8.0.0.5709 Posted: HIPS Content released as PT update.

10:00 GMT on 12-Jun-2014: An EMEA Gold based customer reported a 5709 related issue as a discussion thread on a McAfee internal support distribution list (DL).

10:10 GMT on 12-Jun-2014: Issue identified to be content related by the McAfee Host IPS content team.

11:00 GMT on 12-Jun-2014: McAfee Host IPS content team decides to remediate the content to reduce further potential of customer related issues.

11:30 GMT on 12-Jun-2014: Posting request for remediation content 5710 created.

16:00 GMT on 12-Jun-14: Remediation content 5710 posting to external McAfee updater repositories completed.

19:45 GMT on 12-Nov-2013: SNS Notification and Support Readiness messaging sent out notifying the remediation content posting and reference to reported issue outlined in McAfee Support Knowledge Base article KB82087.