ManageSoft Security Management Data update process

Introduction

This article outlines the process followed by ManageSoft when updating the Security Management Data it publishes. Included is a description and timings of the communications ManageSoft makes to its customers. Many of these updates and notifications occur on the second Tuesday of each month when Microsoft typically publishes new security bulletins, also known as "Patch Tuesday".

MGS-SM-Announce mailing list

ManageSoft uses the MGS-SM-Announce mailing list as the primary vehicle for security related communications to customers. Details on how to subscribe to this and other ManageSoft mailing lists, as well as an archive of prior postings, are available at http://maillist.managesoft.com.

Communications that customers can expect to receive when subscribed to the MGS-SM-Announce mailing list include:
- Notification of updates to files published by ManageSoft
    - windows-errata.cab
    - malwareupdate.cab
    - securityproducts.xml
- Notification of updates to files published by Microsoft
    - wsusscan.cab
    - mssecure_1033.cab
    - invcif.exe
- Notification of updates to ManageSoft Security Bulletin Notes
- Notification of updates to relevant ManageSoft Knowledge Base articles

On Patch Tuesdays, typically the windows-errata.cab update notification is sent within 4 hours of changes being detected on the Microsoft website, and the ManageSoft Security Bulletin Notes notification is sent within 8 hours of changes being detected on the Microsoft website.

All other notification emails are typically sent within 1 day of the update occurring. This includes unannounced changes by Microsoft being detected at other times during the month.

The process in detail

Updates to MBSA and EST security bulletin data

ManageSoft Security Patch Management functionality provides a single centralized interface to manage patches supported by various versions of Microsoft Baseline Security Analyzer and Microsoft Enterprise Scan Tools (ESTs). In order to eliminate the need to manage each tool separately, a windows-errata.cab file is published by ManageSoft containing information about patches supported by these various tools.

ManageSoft continually monitors the Microsoft website for updates to source data about security patches supported by each tool. When an update is detected, the following process is initiated:

1. As soon as an update is detected, the relevant data are automatically downloaded from Microsoft. This includes files such as mssecure_1033.cab for MBSA 1.2 and wsusscan.cab for MBSA 2.0. All new or updated patches are identified and then downloaded, and their details are combined by ManageSoft into the windows-errata.cab file.

2. The windows-errata.cab file is subjected to some basic validation tests, signed, and published on the ManageSoft website. A brief notification email is sent to the MGS-SM-Announce mailing list informing customers that they may now refresh their bulletin data in the ManageSoft Security Patch Management interface and begin packaging and testing the relevant patches. On Patch Tuesdays, customers should avoid attempting to refresh their bulletin data or notify ManageSoft Support of any issues encountered doing a refresh until after this announcement email has been received.

3. The ManageSoft QA team performs testing of the new or updated patches on relevant platforms to ensure that information that has been published by Microsoft is accurate and sufficient to enable correct management of the relevant bulletins with ManageSoft Security Patch Management. Any issues encountered are documented in Security Bulletin Notes at http://www.managesoft.com/support/SecurityBulletinNotes/index.htm, and if necessary, an updated windows-errata.cab file is generated and published.

4. Once full testing has been completed, a further email is sent to the MGS-SM-Announce mailing list documenting full details of the new and updated patches and any relevant known issues.

In cases where the updates from Microsoft are trivial, the two separate emails sent to MGS-SM-Announce noted above may be combined in to one announcement email.

Sometimes security bulletins and patches from Microsoft require an updated securityproducts.xml file to be downloaded and distributed to managed devices. This file contains details used by ManageSoft to detect what software products can be patched are installed on each managed device. If and when that is necessary, this information will be contained within announcements sent to MGS-SM-Announce and the relevant Security Bulletin Notes. See ManageSoft Knowledge Base article 100659 for details on obtaining and deploying the latest securityproducts.xml file.

Updates to Microsoft Office patch data

Microsoft Office patch data are imported directly into ManageSoft Security Patch Management from the invcif.exe file published by Microsoft. Typically this file is updated by Microsoft on Patch Tuesdays. ManageSoft continually monitors the Microsoft website for updates and when an update is detected, the following process is initiated:

1. An email notification is sent to MGS-SM-Announce to notify customers that the .exe file has been updated.

2. The ManageSoft QA team perform testing of the new or updated patches on relevant platforms to ensure that information that has been published by Microsoft is accurate and sufficient to enable correct management of the relevant bulletins with ManageSoft Security Patch Management. Any issues encountered are documented in Security Bulletin Notes at http://www.managesoft.com/support/SecurityBulletinNotes/index.htm.

3. Once full testing has been completed, a further email is sent to the MGS-SM-Announce mailing list documenting full details of the new and updated patches and any relevant known issues.

In cases where the updates from Microsoft are trivial, the two separate emails sent to MGS-SM-Announce noted above may be combined in to one announcement email.

Updates to Microsoft Enterprise Scanning Tools (ESTs)

Microsoft typically releases new or updated Enterprise Scanning Tools (ESTs) within 24 hours of corresponding MBSA 1.2 or MBSA 2.0 data being published. When there is a delay from Microsoft in having an EST available compared to when the source data about bulletins and patches is available, ManageSoft publishes the updated windows-errata.cab file as soon as possible so that customers can begin packaging and testing patches that don't require an EST. Once an EST is available for download, ManageSoft publishes a further update to the windows-errata.cab file. An email notification is sent to MGS-SM-Announce each time the .cab file is updated.

ManageSoft packages containing the latest ESTs available from Microsoft are released via ManageSoft Knowledge Base article 100690.

Updates to malware definition data

ManageSoft routinely updates the malwareupdate.cab file as new instances of malware are identified or revisions are made to the scanning engine. An email notification is sent to MGS-SM-Announce each time the .cab file is updated.

References

1) Microsoft Baseline Security Analyzer product support matrix
http://support.microsoft.com/?scid=kb;en-us;895660

2) ManageSoft Security Bulletin Notes
http://www.managesoft.com/support/SecurityBulletinNotes/index.htm

3) ManageSoft knowledge base article: Updating the Enterprise Scan Tools
http://www.managesoft.com/support/kb/get_item.php?G_ITEM_ID=100690

3) ManageSoft knowledge base article: Updating securityproducts.xml
http://www.managesoft.com/support/kb/get_item.php?G_ITEM_ID=100659

5) ManageSoft windows-errata.cab URL
http://www.managesoft.com/support/SecurityPatchManagement/windows-errata.cab

6) MGS-SM-Announce mailing list URL
http://maillist.managesoft.com