Storwize USB Initialization Tool may contain malicious code

www-01.ibm.com/support/docview.wss

Flashes (Alerts)

Abstract

IBM has detected that some USB flash drives containing the initialization tool shipped with the IBM Storwize V3500, V3700 and V5000 Gen 1 systems contain a file that has been infected with malicious code.

Content

Affected Products
The Initialization Tool on the USB flash drive with the partnumber 01AC585 that shipped with the following System models may have an infected file:
IBM Storwize V3500 - 2071 models 02A and 10A
IBM Storwize V3700 - 2072 models 12C, 24C and 2DC
IBM Storwize V5000 - 2077 models 12C and 24C
IBM Storwize V5000 - 2078 models 12C and 24C

IBM Storwize Systems with serial numbers starting with the characters 78D2 are not affected.

Neither the IBM Storwize storage systems nor data stored on these systems are infected by this malicious code.

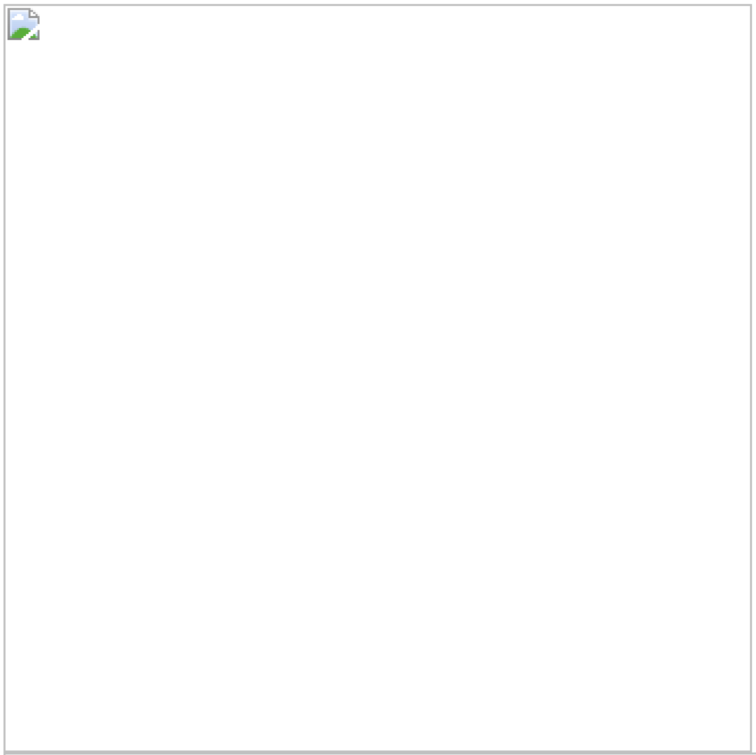
Systems not listed above and USB flash drives used for Encryption Key management are not affected by this issue.

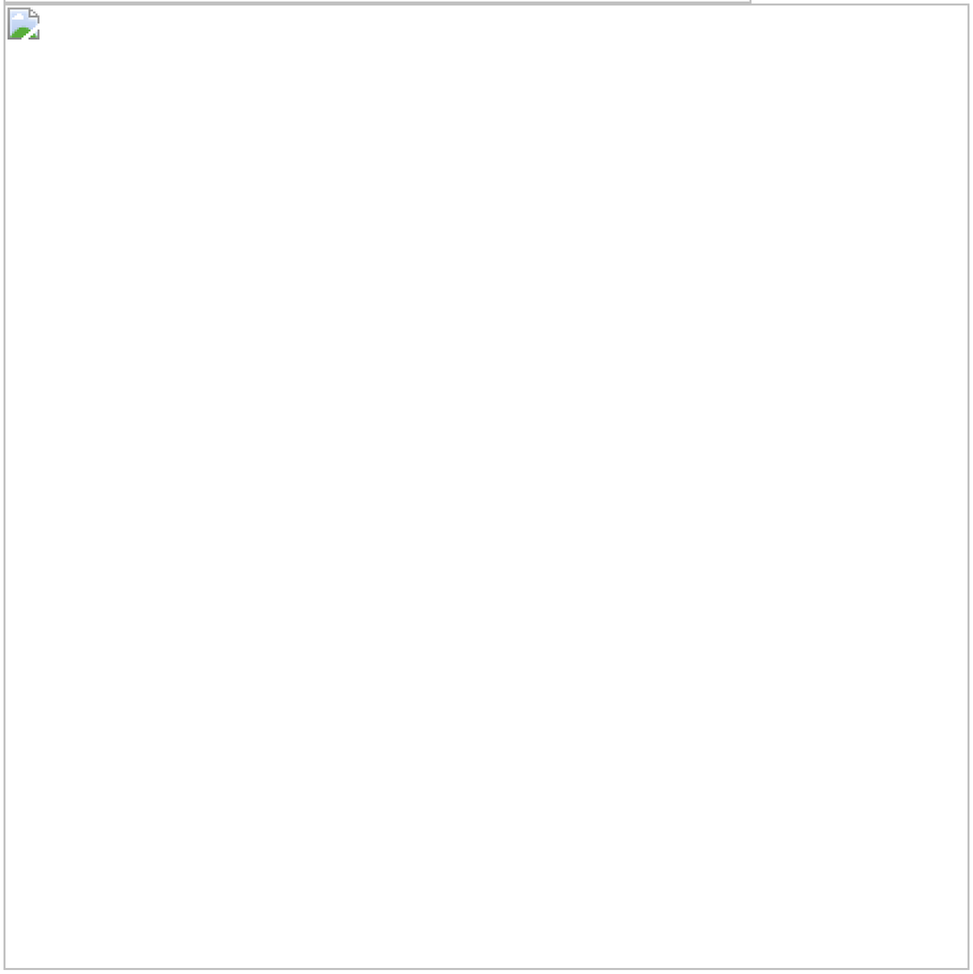
Impact Potential
IBM has identified a malicious file distributed on USB flash drives used in the initialization tool for IBM Storwize V3500, V3700 and V5000 Gen 1 systems.

When the initialization tool is launched from the USB flash drive, the tool copies itself to a temporary folder on the hard drive of the desktop or laptop during normal operation. With that step, the malicious file is copied with the initialization tool to the following temporary folder:
On Windows systems: %TMP%\initTool
On Linux and Mac systems: /tmp/initTool

Important: While the malicious file is copied onto the desktop or laptop, the file is not executed during initialization.

The affected Initialization USB flash drive looks like the images below, and contains a folder called InitTool.





IBM has taken steps to prevent any additional USB flash drives being shipped with this issue.

Client Actions

If you have used the initialization USB flash drive from one of the IBM products listed above and have inserted it into a desktop or laptop to initialize a Storwize system, IBM recommends you verify your antivirus software has already removed the infected file or alternatively remove the directory containing the identified malicious file in the manner described below.

IBM recommends ensuring your antivirus products are updated, configured to scan temporary directories, and issues identified by the antivirus product are addressed.

To manually remove the malicious file, delete the temporary directory:
On Windows systems: %TMP%\initTool
On Linux and Mac systems: /tmp/initTool

In addition for Windows systems, ensure the entire directory is deleted (not moved to the Recycle Bin folder). This can be accomplished by selecting the directory and Shift->Right-click->Delete the directory.
Further, for Initialization Tool USB flash drives, including those that have not yet been used for installation, IBM recommends taking one of the following steps:

1. Securely destroy the USB flash drive so that it can not be reused.
2. Repair the USB flash drive so it can be reused:
    1. Delete the folder called InitTool on the USB flash drive which will delete the folder and all the files inside.If using a Windows machine, holding down shift when deleting the folder will ensure that the files are permanently deleted rather than being copied to the recycle bin.
    2. Download the Initialization tool package from FixCentral https://www.ibm.com/support/fixcentral.
    3. Unzip the package onto the USB flash drive.
    4. Manually scan the USB flash drive with antivirus software.

Further Information

The malicious file has a MD5 hash of 0178a69c43d4c57d401bf9596299ea57.

The malicious file is detected by the following antivirus vendors:

Engine	Signature	Version	Update
AhnLab-V3	Win32/Pondre	3.8.3.16811	20170330
ESET-NOD32	Win32/TrojanDropper.Agent.PYF	15180	20170331
Kaspersky	Trojan.Win32.Reconyc.hvow	15.0.1.13	20170331
McAfee	PWSZbot-FIB!0178A69C43D4	6.0.6.653	20170331

McAfee-GW-Edition	PWSZbot-FIB!0178A69C43D4	v2015	20170331
Microsoft	VirTool:Win32/Injector.EG	1.1.13601.0	20170331
Qihoo-360	Virus.Win32.WdExt.A	1.0.0.1120	20170331
Symantec	W32.Faedevour!inf	1.2.1.0	20170330
Tencent	Trojan.Win32.Daws.a	1.0.0.1	20170331
TrendMicro	PE_WINDEX.A	9.740.0.1012	20170331
TrendMicro-HouseCall	PE_WINDEX.A	9.900.0.1004	20170331
ZoneAlarm	Trojan.Win32.Reconyc.hvow	1	20170331

If you have any questions, contact IBM Support.

[{"Product":{"code":"STLM6B","label":"IBM Storwize V3500 (2071)"},"Business Unit":{"code":"BU054","label":"Systems w\/TPS"},"Component":"--","Platform":[{"code":"PF025","label":"Platform Independent"}],"Version":"Version Independent","Edition":"","Line of Business":{"code":"","label":""}},{"Product":{"code":"STLM6B","label":"IBM Storwize V3500 (2071)"},"Business Unit":{"code":"BU054","label":"Systems w\/TPS"},"Component":" ","Platform":[{"code":"","label":""}],"Version":"","Edition":"","Line of Business":{"code":"","label":""}},{"Product":{"code":"STLM5A","label":"IBM Storwize V3700 (2072)"},"Business Unit":{"code":"BU054","label":"Systems w\/TPS"},"Component":" ","Platform":[{"code":"","label":""}],"Version":"","Edition":"","Line of Business":{"code":"","label":""}},{"Product":{"code":"STHGUJ","label":"IBM Storwize V5000 and V5100"},"Business Unit":{"code":"BU054","label":"Systems w\/TPS"},"Component":" ","Platform":[{"code":"","label":""}],"Version":"","Edition":"","Line of Business":{"code":"","label":""}}]