Initial Publication: 10JAN18

SUMMARY:

The side-channel security vulnerabilities, known as Meltdown and Spectre affect the servers running BackBox in NonStop systems. This document provides procedures for mitigating these security vulnerabilities on any server running BackBox.

The vulnerabilities mitigation requires an update of the Microsoft Windows Server OS on the BackBox server. To have full mitigation, an update of the server system ROM (BIOS) firmware is also required. For the correct update info and the procedure to follow, check the website of the server brand and proceed with the update as specified.

DISCLAIMER:

DETAILED DESCRIPTION:

On January, the 3rd, 2018, side-channel security vulnerabilities involving speculative execution were publicly disclosed by processors manufacturer (Intel, AMD, etc.). The security vulnerabilities, commonly known as Meltdown and Spectre, allow private data to be read.

The servers running BackBox used with NonStop H-series, J-series, and L-series systems are affected by these security vulnerabilities.

The CVSS scores given to these vulnerabilities are:

Scoring system	Base Vector	Base Score
CVE-2017-5715 – aka Spectre, branch target injection		
CVSS version 3.0	AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N	8.2
CVSS version 2.0	AV:A/AC:L/Au:N/C:C/I:P/A:N	6.8
CVE-2017-5753 – aka Spectre, bounds check bypass		
CVSS version 3.0	AV:A/AC:H/PR:L/UI:R/S:C/C:L/I:L/A:L	5.0
CVSS version 2.0	AV:A/AC:M/Au:N/C:P/I:P/A:P	5.4
CVE-2017-5754 – aka Meltdown, rogue data cache load		
CVSS version 3.0	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	7.5
CVSS version 2.0	AV:N/AC:L/Au:N/C:C/I:N/A:N	7.8

For additional information on CVSS, see the Forum for Incident Response and Security Teams (FIRST) documents available on https://www.first.org/cvss.

The CVSS guide describes in detail the above-mentioned scoring system. Base scores range from 0 (lowest intrinsic vulnerability) to 10 (highest intrinsic vulnerability).

Intel Security Advisory INTEL-SA-00088 describes the security vulnerabilities affecting specific Intel x86 processors - https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr

For x86 servers running Microsoft Windows OS, Microsoft has released OS patches and procedures to mitigate the security vulnerabilities. Microsoft Security Advisory ADV180002 provides an overview of the vulnerabilities mitigation - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

The full vulnerabilities mitigation also requires a server system ROM (BIOS) firmware update. Please refer to your server manufacturer for the correct update and for the procedure to follow in order to apply the update.

ADDITIONAL BACKGROUND INFORMATION:

The NIST National Vulnerability Database references are –
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2017-5715
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2017-5753
https://web.nvd.nist.gov/view/vuln/detail?vulnID=CVE-2017-5754

AFFECTED PRODUCTS:

Any Intel x86 processors equipped Server running BackBox product.

PROCEDURE:

Overview:

The main steps of the BackBox server vulnerability mitigation procedure are:

1. Update Microsoft Windows Server OS and Internet Explorer 11
2. If needed, update anti-virus to be compatible with Windows Server and Internet Explorer changes
3. Update the server System ROM firmware according to the manufacturer instructions of your server
4. Configure Microsoft OS registry settings to enable the mitigations
5. Verify that protections are enabled

The BackBox server will be taken offline during/before the procedure.

Steps 1 thru 5 take 20 to 45 minutes to complete; the BackBox server must be restarted.

Step 1:

Background:

As a general rule, a BackBox server running Windows Server 2008 R2 or Windows Server 2012 R2 should be patched on a monthly basis or when critical security vulnerabilities - like the Intel side-channel analysis - are mitigated.

Procedure:

For the Intel side-channel analysis vulnerability mitigation, update the Windows OS with the patch described in Microsoft Knowledge Base article 4072698 - https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution.

NOTE: Microsoft Knowledge Base article 4072698 contains CLI commands to be used in Step 5 below. Suggest printing out this article for use in Step 5 below.

In the Microsoft Knowledge Base article 4072698, navigate to the Microsoft Knowledge Base article for the Windows Server version running on BackBox server. Download the standalone package for the update from the Microsoft Update Catalog website, using the link in the article, and copy the package to the BackBox server.

Double-click on the package and install the OS update.

NOTE: At the completion of the OS update install, a prompt requests to restart the server. The server restart can wait until after Step 4 below until the update of the server System ROM has been completed. Delaying the restart saves the time required for an extra server restart.

The Microsoft Security Advisory ADV180002 states to update Internet Explorer 11.

For Windows Server 2008 R2 and Windows Server 2012 R2, use the patch

described in Microsoft Knowledge Base article KB4056568 – https://support.microsoft.com/en-us/help/4056568/cumulative-security-update-for-internet-explorer.

For Windows Server 2016, use the patch described in Microsoft Knowledge Base article KB4056890 – https://support.microsoft.com/en-us/help/4056890/windows-10-update-kb4056890.

Step 3:

Make sure to have installed the updated anti-virus versions compatible the latest Windows Server and with Internet Explorer 11 changes.

Step 4:

Procedure:

Identify your manufacturer and server model running the BackBox software. Download the appropriate System ROM or BIOS upgrade according to your server manufacturer instructions and follow the provided upgrade procedure.

After the completion of the System ROM update install, accept the request to restart the server. The server will reboot with the updated OS with the mitigation fix and the updated System ROM with the new Intel micro-code.

Step 5:

Background:

After the BackBox server has been rebooted with the updated OS and the updated System ROM, the server needs to be configured to enable the mitigations for the side-channel analysis security vulnerability as described in Microsoft Knowledge Base article 4072698. This article was referenced in Step 2 above.
See step 2 for the link, if you have not printed out this article for reference.

NOTE: The Microsoft Knowledge Base article 4072698 states that enabling the mitigations for the side-channel analysis security vulnerability may affect performance.

Procedure:

In the Microsoft Knowledge Base article 4072698, go to the section with the heading “Enabling protections on the server”.

WARNING: This section contains steps that modify the Windows Server OS registry. Serious problems can occur if the registry is modified incorrectly. Take extra care in following the steps in this section.

For added protection, back up the registry before making any modifications. This will allow the registry to be restored to the state before the modifications were made. For information on how to back up and restore the registry, see Microsoft Knowledge Base article 322756 – https://support.microsoft.com/en-us/help/322756/how-to-back-up-and-restore-the-registry-in-windows

Open a command prompt window and enter the registry settings modification commands as shown in the section to enable the mitigations. After entering the registry set commands, restart the server for the registry changes to take effect.

Step 6:

Procedure:

In the Microsoft Knowledge Base article 4072698, go to the section with the heading “Verifying that protections are enabled”.

Follow the appropriate procedure for the Windows Server version to verify if the protections are enabled, by comparing the actual output to the output shown in the article.

PROCEDURE END