Meltdown and Spectre vulnerability

Jan 12

2018

Product Security Advisory

Product Security Advisory: Meltdown and Spectre vulnerability in IT-Products

Background:

In December 2017 information about two vulnerabilities in modern processors were published. These exploits are often referred to as Meltdown and Spectre. A large proportion of current IT-products are potentially affected – including systems with Intel-based processors. In order to use the exploit, an attacker needs to execute malicious code on the target system. For this reason it is advised to protect systems from unauthorized access (e.g. by using a strong password policy). In addition potentially affected systems should be patched with latest security updates, in order to reduce the attack surface.

The following Bosch and HP Video system products include Intel-based processors and are considered vulnerable:

Storage devices: DIVAR IP 2000, DIVAR IP 3000, DIVAR IP 5000, DIVAR IP 6000, DIVAR IP 7000

Decoder: VIDEOJET decoder 8000

IT-equipment: HP Workstation, HP Server

Please note the provided solution guidance for the products as follows:

DIVAR IP 2000, DIVAR IP 5000 and VIDEOJET decoder 8000

Firmware updates will be published shortly. Download links will be published in the product catalogue and on the Bosch Security Systems DownloadStore:

https://downloadstore.boschsecurity.com/

DIVAR IP 3000

- press CTRL+ALT+DEL, then hold down SHIFT while clicking the Switch User option and keep SHIFT pressed for about five seconds.
- Log in using the BVRAdmin account
- Enable Windows Update in the Control Panel and install latest Updates (preferred)
  Note: it may be required to enable the *Windows Update* service under services first
- Alternatively patch KB4056897 can be downloaded and installed on the system
  http://download.windowsupdate.com/d/msdownload/update/software/secu/2018/01/windows6.1-kb4056897-x64_2af35062f69ce80c4cd6eef030eda31ca5c109ed.msu

DIVAR IP 6000 (current generation DIP-61x)

- Log in using the BVRAdmin account
- Enable Windows Update in the Control Panel and install latest Updates (preferred)
- Alternatively patch KB4056898 can be downloaded and installed on the system
  http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows8.1-kb4056898-v2-x64_754f420c1d505f4666437d06ac97175109631bf2.msu

DIVAR IP 7000 (current generation DIP-71x)

- press CTRL+ALT+DEL, then hold down SHIFT while clicking the Switch User option and keep SHIFT pressed for about five seconds.
- Log in using the BVRAdmin account
- Enable Windows Update in the Control Panel and install latest Updates (preferred)
- Alternatively patch KB4056898 can be downloaded and installed on the system
  http://download.windowsupdate.com/c/msdownload/update/software/secu/2018/01/windows8.1-kb4056898-v2-x64_754f420c1d505f4666437d06ac97175109631bf2.msu

HP Workstations, HP Servers and PC-based products which are already end-of-life

- Log in using the administrative account
- Enable Windows Update in the Control Panel and install latest Updates (preferred)
- Or download and install the matching patch from Microsoft:
  Windows 7 or Window (Storage) Server 2008 R2
  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056897
  Windows 8.1 or Window (Storage) Server 2012 R2
  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056898
  Windows 10
  https://www.catalog.update.microsoft.com/Search.aspx?q=KB4056891

Note: This article will be updated, if additional patches or guidelines are published by the CPU or OS vendor. First tests indicated that patched systems still operate within the given specification – despite potential performance impacts related to the listed security patches.