Secunia Advisory ID	SA80899
Title	VMware ESXi CPU Speculative Executions Security Bypass Vulnerability
Release date	2018-01-04
Last update	2018-01-23
Criticality	- Not critical
Impact	Security Bypass
Where	Local system
Solution Status	Vendor Patched
Secunia CVSS Scores	Base: 1.7 , Overall: 1.3 (AV:L/AC:L/Au:S/C:P/I:N/A:N/E:U/RL:OF/RC:C)
CVE references	CVE-2017-5753 |

Affected operating system and software

Operating systems

VMware ESXi 5.x

Advisory Details:

Description:

A vulnerability has been reported in VMware ESXi, which can be exploited by malicious, local users in a guest virtual machine to bypass certain security restrictions.

For more information:
SA80843 (#1)

The vulnerability is reported in version 5.5.

Solution:

Apply ESXi550-201801301-BG.

Original advisory:

VMware (VMSA-2018-0002, VMSA-2018-0002.1, VMSA-2018-0002.2, VMSA-2018-0002.3):
https://www.vmware.com/security/advisories/VMSA-2018-0002.html

References:

SA80843:
SA80843

Changelog:

2018-01-23: Updated the "Solution" section due to an update of the vendor's advisory. Updated the solution status. Updated the tags in the "Original Advisory" section.
2018-01-17: Updated the "Solution" section due to an update of the vendor's advisory. Updated the solution status. Updated the tags in the "Original Advisory" section.
2018-01-09: Updated "Solution" section due to release of vendor patch. Updated the solution status. Updated the tags in the "Original Advisory" section.
2018-01-04: Initial release