[SA80900] Citrix XenServer Multiple Vulnerabilities

Secunia Advisory ID	SA80900
Title	Citrix XenServer Multiple Vulnerabilities
Release date	2018-01-05
Last update	2018-01-05
Criticality	- Not critical
Impact	Exposure of sensitive information, DoS
Where	Local system
Solution Status	No Fix
Secunia CVSS Scores	Base: 4.6 , Overall: 3.9 (AV:L/AC:L/Au:S/C:N/I:N/A:C/E:U/RL:U/RC:C)
CVE references	CVE-2017-5715 | CVE-2017-5754 |

Affected operating system and software

Operating systems

Citrix XenServer 6.0

Citrix XenServer 6.2

Citrix XenServer 6.5

Advisory Details:

Description:

Multiple vulnerabilities have been reported in Citrix XenServer, which can be exploited by malicious, local users to disclose sensitive information and cause a DoS (Denial of Service).

For more information:
SA80843 (#2 and #3)

1) An error related to x86 PV guests accessing internally used pages can be exploited to cause a crash of the host system.

2) An error related to x86 shadow mode refcount overflow check can be exploited to cause a crash of the host system.

3) An error related to x86 shadow mode refcount error handling can be exploited to cause a crash of the host system.

4) An error related to x86 log-dirty handling can be exploited to cause a crash of the host system.

The vulnerabilities are reported in versions 6.5, 6.2.0, and 6.0.2.

Solution:

No official solution is currently available.

Provided and/or discovered by:

1-4) Reported by the vendor

Original advisory:

https://support.citrix.com/article/CTX231390

References:

SA80843:
SA80843

Changelog:

2018-01-05: Initial release