[SA80103] VMware Workstation Multiple Vulnerabilities

Secunia Advisory ID	SA80103
Title	VMware Workstation Multiple Vulnerabilities
Release date	2017-11-17
Last update	2018-01-04
Criticality	- Less critical
Impact	Exposure of sensitive information, Security Bypass, System access, Privilege escalation, DoS
Where	From local network
Solution Status	Vendor Patched
Secunia CVSS Scores	Base: 7.7 , Overall: 5.7 (AV:A/AC:L/Au:S/C:C/I:C/A:C/E:U/RL:OF/RC:C)
CVE references	CVE-2017-4933 | CVE-2017-4934 | CVE-2017-4936 | CVE-2017-4938 | CVE-2017-4937 | CVE-2017-5753 | CVE-2017-5715 | CVE-2017-4941 | CVE-2017-4935 |

Affected operating system and software

Software

VMware Workstation 12.x

Advisory Details:

Description:

Multiple vulnerabilities have been reported in VMware Workstation, which can be exploited by malicious, local users in a guest virtual machine to disclose potentially sensitive information, bypass certain security restrictions, cause a DoS (Denial of Service), and gain escalated privileges, by malicious, local users to cause a DoS, and by malicious users to compromise a vulnerable system.

For more information:
SA80843 (#1 and #2)

1) An error when handling the NAT IP Fragment Reassembly can be exploited to cause a heap-based buffer overflow.

2) An error in the JPEG2000 parser within the TPView.dll module can be exploited to cause an out-of-bounds write memory access.

3) An error in the JPEG2000 parser within the TPView.dll module can be exploited to cause an out-of-bounds read memory access.

4) Another error in the JPEG2000 parser within the TPView.dll module can be exploited to cause an out-of-bounds read memory access.

Successful exploitation of vulnerabilities #2 through #4 requires virtual printing to be enabled and a Windows host.

5) An error when handling guest RPC requests can be exploited to trigger a NULL-pointer dereference and subsequently cause a crash in guest.

6) A type confusion error related to VNC can be exploited to cause a stack-based buffer overflow by sending specially crafted VNC packets.

7) An error related to VNC can be exploited to cause a heap-based buffer overflow by sending specially crafted VNC packets.

Successful exploitation of the vulnerabilities #6 and #7 may allow execution of arbitrary code, but requires privileges for an active VNC session.

The vulnerabilities are reported in versions prior to 12.5.8.

Solution:

Update to version 12.5.8.

Provided and/or discovered by:

1) Jun Mao, Tencent PC Manager via ZDI.
2) An anonymous person via ZDI.
6) Lilith Wyatt and an anonymous person, Cisco Talos.
7) Lilith Wyatt, Cisco Talos.

The vendor credits:
3, 4) Ke Liu, Tencent's Xuanwu Lab.
5) Skyer.

Original advisory:

VMware (VMSA-2018-0002):
https://www.vmware.com/security/advisories/VMSA-2018-0002.html
Cisco Talos:
https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0368
VMware (VMSA-2017-0018):
https://www.vmware.com/security/advisories/VMSA-2017-0018.html
http://www.zerodayinitiative.com/advisories/ZDI-17-921/
https://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0369
ZDI-17-922:
http://www.zerodayinitiative.com/advisories/ZDI-17-922/
VMware (VMSA-2017-0021):
https://www.vmware.com/security/advisories/VMSA-2017-0021.html

References:

SA80843:
SA80843

Changelog:

2018-01-04: Added further vulnerabilities. Updated the "Description" section. Updated impacts, vulnerability count, and CVE references. Added links to the "Original Advisory" and "Other References" sections.
2017-12-20: Updated the vulnerabilities #6 and #7 due to new known details. Updated credits. Added a links to the "Original Advisory" section.
2017-12-19: Updated advisory to include vulnerabilities #6 and #7. Increased vulnerability count. Added CVE-2017-4941 and CVE-2017-4933 to the list of CVE identifiers. Updated CVSS2 score, impacts, vector, and credits. Added link to the "Original Advisory" section.
2017-11-21: Updated the vulnerability #1 due to new known details. Updated credits. Added a link to the "Original Advisory" section.
2017-11-21: Updated credits. Added link to the "Original Advisory" section.
2017-11-17: Initial release