PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Microsoft Edge Remote Code Execution Vulnerability	Microsoft Edge is prone to remote code execution vulnerability due to the way that the Chakra JavaScript engine renders when handling objects in memory.	Version(s): Any	Published - June 14,2016 CVE-2016-3202 CVSS - 9.3 Vendor's Advisory Available at : https://technet.microsoft.com/library/security/ms16-068
Adobe AIR Remote Host Privileges Vulnerability	Adobe AIR Desktop Runtime 21.0.0.215 and earlier is prone to a vulnerability in the directory search path used by the AIR installer. Successful attacks could allow attackers to take control over the system.	Version(s): prior to21.0.0.215	Published - June 16, 2016 CVE-2016-4126 CVSS - 9.3 Vendor's Advisory Available at: https://helpx.adobe.com/security/products/air/apsb16-23.html
Microsoft Multiple Office Products Remote Code Execution via a Crafted Office File	Microsoft Word 2007 SP3, 2013 SP1, 2016 and 2010 SP2, Office 2010 SP2 and 2016, Word 2011 and 2016 for Mac, Office Compatibility Pack SP3, Word Automation Services on Microsoft SharePoint Server 2010 SP2 and 2013 SP1, Office Web Apps 2010 SP2, Office Web Apps Server 2013 SP1 and Office Online Server allow remote attackers to execute arbitrary code via a crafted Office file.	Version(s) :prior to 2016	Published - June 14 2016 CVE-2016-0025 CVSS - 9.3 Vendor's Advisory Available at: https://technet.microsoft.com/library/security/ms16-070
SAP Documentation and Translation Tools Remote Code Injection Vulnerability	SAP Documentation and Translation Tools is prone to remote code injection vulnerability. Successful exploits enable attacker to access arbitrary files and directories located in an SAP server filesystem including application source code, configuration, and system files. SAP released Security Note 2306709 to address the issue.	Version(s) :ANY	Published - Jun 14 2016 SBV-60337 CVSS - 9.3 The vendor's advisory is available at: https://erpscan.com/press-center/blog/sap-security-notes-june-2016/
QEMU Local DoS or Arbitrary Code Execution by Guest OS Administrators	The (1) esp_reg_read and (2) esp_reg_write functions in hw/scsi/esp.c in QEMU allow local guest OS administrators to cause a denial of service (QEMU process crash) or execute arbitrary code on the QEMU host via vectors related to the information transfer buffer.	Version(s) : ANY	Published -Jun 14 2016 CVE-2016-5338 CVSS - 5.7 Vendor's Advisory Available at https://lists.gnu.org/archive/html/qemu-devel/2016-06/msg01507.html
SolarWinds Virtualization Manager 6.3.1 and Earlier Remote Code Execution in the RMI Service	The RMI service in SolarWinds Virtualization Manager 6.3.1 and earlier allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library	Version(s) :prior to 6.3.1	Published -Jun 7 2016 CVE-2016-0678 CVSS - 10 The vendor's advisory is available at: Block the network access to the host at the relevant port, by adding an access rule to the appropriate firewall(s) Remove or shutdown the service/product, in case it is not needed Shield the vulnerability by enabling an IPS signature, if available
Google Chrome before 51.0.2704.103 Remote Unspecified Vulnerability	Google Chrome before 51.0.2704.103 is prone to remote unspecified vulnerability.	Version(s)prior to 51.0.2704.103	Published - June 16 2016 CVE-2016-1704 CVSS - 8.2 Vendor's Advisory Available at http://rhn.redhat.com/errata/RHSA-2016-1262.html Upgrade to latest google chrome
ClamAV <=0.99.2 Remote Code Execution Vulnerability via SCAN Command	ClamAV version 0.99.2 and earlier is prone to a remote code execution vulnerability via the SCAN command. This vulnerability was published by Qualys	Version(s) Prior to 0.99.2	Published - June 12 2016 SBV-60457 CVSS - 7.5 Vendor's Advisory Available at Block the network access to the host at the relevant port, by adding an access rule to the appropriate firewall(s) Remove or shutdown the service/product, in case it is not needed Shield the vulnerability by enabling an IPS signature, if available
Libav before 11.7 Remote DoS or Code Execution via a Crafted MP4 File	The mov_read_dref function in libavformat/mov.c in Libav before 11.7 allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via the entries value in a dref box in an MP4 file.	Version(s):Prior to 11.7	Published - June 15 2016 CVE-2016-3062 CVSS - 6.8 Vendor's Advisory Available : Upgrade to latest Libav to version 11.47 or later
Cisco RV Series Routers Remote Arbitrary Code Execution Vulnerability	Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN and Cisco RV215W Wireless-N VPN Routers allow a remote attacker to execute arbitrary code with root level privileges due to a flaw in their web interfaces. The flaw allows an attacker to send a crafted http request which is not validated adequately.	Version(s): RV series Routers prior to 1.3.0.8,1.0.3.16,1.2..1.7	Published -Jun 15 2016 CVE-2016-1395 CVSS - 10.0 Vendor's Advisory Available http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160615-rv
Apache Struts 2.3.20 through 2.3.28.1 Remote Code Execution via a Crafted Expression	Apache Struts 2.3.20 through 2.3.28.1 allows a remote attacker to execute arbitrary code via a crafted expression related to the REST plugin.	Version(s): 2.3.2.0 - 2.3.28.1	Published -Jun 17 2016 CVE-2016-4438 CVSS - 7.5 Vendor's Advisory Available at https://struts.apache.org/docs/s2-037.html