MINISTRY OF
HOME AFFAIRS
CAYMAN ISLANDS GOVERNMENT

National Cyber Awareness System:

Vulnerability Summary for the Week of March 7, 2016

03/15/2016

Original release date: March 14, 2016

Below is a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- digital_editions	Adobe Digital Editions before 4.5.1 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	2016-03-09	10.0	CVE-2016-0954
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic	2016-03-09	10.0	CVE-2016-1007

	before 15.006.30121, and Acrobat and Acrobat Reader DC Continuous before 15.010.20060 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1009.			
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic before 15.006.30121, and Acrobat and Acrobat Reader DC Continuous before 15.010.20060 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1007.	2016-03-09	10.0	CVE-2016-1009
adobe -- acrobat	Untrusted search path vulnerability in Adobe Reader and Acrobat before 11.0.15, Acrobat and Acrobat Reader DC Classic before 15.006.30121, and Acrobat and Acrobat Reader DC Continuous before 15.010.20060 on Windows and OS X allows local users to gain privileges via a Trojan horse DLL in an unspecified directory.	2016-03-09	7.2	CVE-2016-1008
microsoft -- .net_framework	Microsoft .NET Framework 2.0 SP2, 3.0 SP2, 3.5, 3.5.1, 4.5.2, 4.6, and 4.6.1 mishandles signature validation for unspecified elements of XML documents, which allows	2016-03-09	10.0	CVE-2016-0132

	remote attackers to spoof signatures via a modified document, aka ".NET XML Validation Security Feature Bypass."			
microsoft infopath	--	Microsoft InfoPath 2007 SP3, 2010 SP2, and 2013 SP1 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	2016-03-09	9.3	CVE-2016-0021
microsoft windows	--	OLE in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted file, aka "Windows OLE Memory Remote Code Execution Vulnerability," a different vulnerability than CVE-2016-0091.	2016-03-09	9.3	CVE-2016-0092
microsoft windows	--	Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 allow remote attackers to execute arbitrary code via crafted media content, aka "Windows Media Parsing Remote Code Execution Vulnerability."	2016-03-09	9.3	CVE-2016-0098
microsoft windows	--	Microsoft Windows Server 2008 R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow remote attackers to	2016-03-09	9.3	CVE-2016-0101

	execute arbitrary code via crafted media content, aka "Windows Media Parsing Remote Code Execution Vulnerability."			
microsoft -- windows	The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrary code via a crafted PDF document, aka "Windows Remote Code Execution Vulnerability."	2016-03-09		

Source: US-CERT
