solarwinds msp

Security Scan

Assessment completed on: 2017-01-31T23:03:16Z

IP: 192.168.2.121 Hostname: dc5750-04.communica.local OS: Windows Vista

Vulnerability Summary

FAIL

Vulnerability Count by Severity

High: 5
Medium: 3
Low: 0

Percentage of Vulnerabilities by Vendor

Vendor	%
Microsoft	83%
Adobe	16%

Vulnerability by Vendor Details

Each vulnerability is assigned a severity level of High, Medium, or Low, which is based on the CVSS scoring system.

Severity	CVSS Score
High	7.0 - 10.0
Medium	4.0 - 6.9
Low	0.0 - 3.9

Microsoft

How to fix: *Run Windows Update to ensure you have the latest patches installed. Windows Update should be set to receive updates for 'Windows and other products from Microsoft Update.'*

Title:	Website spoofing vulnerability in Microsoft Internet Explorer via a crafted HTML document
Check ID:	oval:org.secpod.oval:def:9072
CVSS:	4.0
References:	CVE-2013-1451
Title:	Multiple unspecified vulnerabilities in Microsoft Internet Explorer by leveraging access to a Low integrity process

Check ID:	oval:org.secpod.oval:def:5219
CVSS:	5.8
References:	CVE-2012-1545
Title:	Information disclosure vulnerability in Microsoft Internet Explorer via a crafted HTML document
Check ID:	oval:org.secpod.oval:def:9073
CVSS:	4.0
References:	CVE-2013-1450
Title:	MS13-002 - Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (XML 4.0)
Check ID:	lua:com.iscanonline:def:5810
CVSS:	9.3
References:	CVE-2013-0007, MS13-002
Title:	MS12-043 - Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (XML 4.0)
Check ID:	lua:com.iscanonline:def:5889
CVSS:	9.3
References:	CVE-2012-1889, MS12-043

Adobe

How to fix: *Run the affected software's update mechanism, or go to the vendor's site to download the latest version and/or patches.*

Title:	APSB16-02 - Security Update - Adobe Reader 11.0.14 released
Check ID:	lua:com.iscanonline:def:6457
CVSS:	10.0
References:	CVE-2016-0931, CVE-2016-0932, CVE-2016-0933, CVE-2016-0934, CVE-2016-0935, CVE-2016-0936, CVE-2016-0937, CVE-2016-0938, CVE-2016-0939, CVE-2016-0940, CVE-2016-0941, CVE-2016-0942, CVE-2016-0943, CVE-2016-0944, CVE-2016-0945, CVE-2016-0946, CVE-2016-0947, APSB16-02

Network Port Details

This section displays the open and listening TCP/IP ports on this system. Open ports indicate that a service is listening for external communication from a remote computer. Review the list of open ports to determine if they are absolutely necessary. Disable any unnecessary services to reduce the risk of compromise from malware or attackers. We recommend that you back up your system before making any changes. Your local IT administrator will be able to provide you with guidance on managing your network ports.

Result			
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5357	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49156	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49248	0.0.0.0:0	LISTENING
TCP	127.0.0.1:5939	0.0.0.0:0	LISTENING
TCP	192.168.2.121:139	0.0.0.0:0	LISTENING
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:3389	[::]:0	LISTENING
TCP	[::]:5357	[::]:0	LISTENING
TCP	[::]:49152	[::]:0	LISTENING
TCP	[::]:49153	[::]:0	LISTENING
TCP	[::]:49154	[::]:0	LISTENING
TCP	[::]:49156	[::]:0	LISTENING
TCP	[::]:49248	[::]:0	LISTENING