solarwinds msp

Expanded Data Breach Scan

Assessment completed on: 2018-06-18T22:50:58Z

IP: 192.168.2.195 Hostname: 6000pro-01.communica.local OS: Windows 7

Unprotected Data Summary

FAIL

Unprotected Data Count by Type

Personal ID (SWE)	5

Potential Liability

Kr 2,500.00

Elapsed Time	0 hours, 17 minutes, 47 seconds
Files Scanned	11,803
Files with Violation	3
Total Violations	5

Vulnerability Summary

FAIL

Vulnerability Count by Severity

High: 3
Medium: 1
Low: 0

Percentage of Vulnerabilities by Vendor

Vendor	%
Microsoft	100%

Technical Safeguards Summary

FAIL

Compliant	Not Compliant
10	8

Technical Safeguards Details

Check ID:	lua:com.iscanonline:def:5002	✗
Title:	MSS: Screen Saver Grace Period (0 seconds)	
Description:	The Screen Saver Grace Period is the interval (in seconds) between screen saver activation and the requirement of a password to unlock the screen saver. (NOTE: This is not the same as the Screen Saver Timeout value.)	
Check ID:	lua:com.iscanonline:def:8170	✓
Title:	Antivirus Policy: Verify antivirus software installed	
Description:	This check determines whether any antivirus software is installed.	
Check ID:	lua:com.iscanonline:def:5007	✗
Title:	Password Policy: Minimum password length (7 characters or more)	
Description:	Minimum password length is the least number of characters required for a user password.	
Check ID:	lua:com.iscanonline:def:5000	✓
Title:	Power Management: Require a password when a computer wakes - On Battery (Enabled)	
Description:	This policy setting determines whether a password is required when resuming from sleep, while on battery power.	
Check ID:	lua:com.iscanonline:def:5019	✗
Title:	Account Lockout Policy: Account lockout duration (30 minutes or longer)	
Description:	Account lockout duration is the amount of time (in minutes) a locked-out account remains locked out before automatically becoming unlocked.	
Check ID:	lua:com.iscanonline:def:5005	✗
Title:	Password Policy: Enforce password history (4 passwords or more)	
Description:	Password history is the number of unique new passwords that have to be associated with a user account before an old password can be reused.	
Check ID:	lua:com.iscanonline:def:5006	✓
Title:	Password Policy: Maximum password age (90 days or less)	
Description:	Maximum password age is the period of time (in days) that a password can be used before the system requires the user to change it.	
Check ID:	lua:com.iscanonline:def:5003	✗

Title:	Remote Desktop Services: Set time limit for active but idle Remote Desktop / Terminal Services sessions (15 minutes or less)	
Description:	This time limit is the maximum amount of time (in minutes) that an active Remote Desktop / Terminal Services session can be idle (without user input) before it is automatically disconnected.	
Check ID:	lua:com.iscanonline:def:5008	✗
Title:	Password Policy: Password must meet complexity requirements (Enabled)	
Description:	Password complexity determines whether numbers, uppercase letters, and non-alphabetic characters are required for user passwords.	
Check ID:	lua:com.iscanonline:def:5018	✗
Title:	Account Lockout Policy: Account lockout threshold (6 attempts or less)	
Description:	Account lockout threshold is the number of failed logon attempts that causes a user account to be locked out.	
Check ID:	lua:com.iscanonline:def:5004	✗
Title:	Remote Desktop Services: Set time limit for disconnected sessions (1 minute)	
Description:	This time limit is the maximum amount of time (in minutes) that a disconnected session is kept active on the server.	
Check ID:	lua:com.iscanonline:def:5001	✓
Title:	Power Management: Require a password when a computer wakes - Plugged In (Enabled)	
Description:	This policy setting determines whether a password is required when resuming from sleep, while plugged in.	
Check ID:	lua:com.iscanonline:def:5068	✓
Title:	Screen Saver Policy: Screen Saver is password protected (Enabled)	
Description:	This check verifies the screen saver is password protected.	
Check ID:	lua:com.iscanonline:def:5066	✓
Title:	Account Policy: Inactive user accounts (more than 90 days)	
Description:	This check determines whether there are any inactive users on the machine.	
Check ID:	lua:com.iscanonline:def:5069	✓
Title:	Screen Saver Policy: Screen Saver timeout (15 minutes or less)	
Description:	Screen Saver timeout is the amount of time (in minutes) the system will remain idle before the screen saver starts.	
Check ID:	lua:com.iscanonline:def:5067	✓
Title:	Screen Saver Policy: Screen Saver (Enabled)	
Description:	This check verifies a screen saver is enabled.	
Check ID:	lua:com.iscanonline:def:8172	✓
Title:	Antivirus Policy: Verify antivirus software enabled and up-to-date	
Description:	This check determines whether the installed antivirus software is enabled and up-to-date.	

Check ID:	lua:com.iscanonline:def:8171
Title:	Firewall Policy: Verify firewall software installed and running
Description:	This check determines whether any firewall software is installed and running.

Unprotected Data Details

The findings data from your scan has been reduced to the following amounts where necessary:

Suspected Instances: 400
Findings per Instance: 50
Folders per PST File: 50
Messages per PST Folder: 100
Files per ZIP File: 100

File Name	Findings Count
C:\Stor-1\Documents and Settings\All Users\Documents\Familjepärm.doc	3

SHA256	e48bd9d5fd698f7afcdd34432f40a72330e2eea5656139b7b00a4a5c0c8ae0c6
SHA1	6616af8360c7b68895ae2c4d92c340cfc9849e42
MD5	ab9c61fc871b38f906dd2b872baaecd7

Personal ID (SWE)

960XXXXXX44

980XXXXXX38

660XXXXXX06

C:\Users\William.COMMUNICA\Downloads\Inkomstdeklaration 2016 Robert Ingram.pdf	1

SHA256	f7b0a4c1486ac65b8c1018938b53b18e5345d0930f95a0052faf8a615ccb5b87
SHA1	ba46a041ae42eaec39998338d56e33986ae56fbd
MD5	c3798ddc81c61971f23bcb77cb2e72dd

Personal ID (SWE)

980XXXXXX38

C:\Users\William.COMMUNICA\Downloads\Sparkontoavtal.pdf	1

SHA256	ad99734a2211d8e38beca8795f9e95038011b6e4e517affb7b18919073620221
SHA1	f810ffcd245020d55fc5f24708ed69bc85f5e2c1
MD5	4f73d597978bd30cd101ecf9d4f8cffb

Personal ID (SWE)

670XXXXXX92

Unprotected Data Scan Statistics

Elapsed Time	0 hours, 17 minutes, 47 seconds
Files Scanned	11,803
Files with Suspect Data	3
Bytes Scanned	1,448,387,349
Suspected Instances Found	5

Volumes Scanned

Drive Root	Drive Capacity	Used Space	Free Space
D:\	5,242,875,904	4,512,186,368	730,689,536
C:\	104,182,312,960	55,230,631,936	48,951,681,024

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:	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
Title:	KB4022150 - Security Update for Microsoft Office Compatibility Pack SP3

Check ID:	lua:com.iscanonline:def:8442
CVSS:	9.3
References:	CVE-2018-8147, CVE-2018-8148, KB4022150
Title:	KB4018308 - Security Update for Microsoft Office Viewers and Office Compatibility Pack
Check ID:	lua:com.iscanonline:def:8441
CVSS:	4.3
References:	CVE-2018-8160, KB4018308

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	0.0.0.0:664	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	0.0.0.0:5948	0.0.0.0:0	LISTENING
TCP	0.0.0.0:16993	0.0.0.0:0	LISTENING
TCP	0.0.0.0:17500	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	0.0.0.0:54402	0.0.0.0:0	LISTENING
TCP	0.0.0.0:54416	0.0.0.0:0	LISTENING
TCP	0.0.0.0:54427	0.0.0.0:0	LISTENING
TCP	0.0.0.0:54475	0.0.0.0:0	LISTENING
TCP	0.0.0.0:54478	0.0.0.0:0	LISTENING
TCP	0.0.0.0:54560	0.0.0.0:0	LISTENING
TCP	127.0.0.1:843	0.0.0.0:0	LISTENING
TCP	127.0.0.1:17600	0.0.0.0:0	LISTENING
TCP	127.0.0.1:44430	0.0.0.0:0	LISTENING
TCP	127.0.0.1:49182	0.0.0.0:0	LISTENING
TCP	192.168.2.195:139	0.0.0.0:0	LISTENING
TCP	[::]:135	[::]:0	LISTENING
TCP	[::]:445	[::]:0	LISTENING
TCP	[::]:3389	[::]:0	LISTENING
TCP	[::]:5357	[::]:0	LISTENING
TCP	[::]:17500	[::]:0	LISTENING
TCP	[::]:49152	[::]:0	LISTENING
TCP	[::]:49153	[::]:0	LISTENING
TCP	[::]:49154	[::]:0	LISTENING
TCP	[::]:54402	[::]:0	LISTENING
TCP	[::]:54416	[::]:0	LISTENING
TCP	[::]:54560	[::]:0	LISTENING