Scan Date
12/01/15
SAMPLE
Windows
Workstation
Assessment

Data Breach Risk Analysis Report & Vulnerability Summary

Note:
Partial Report 8 pages of 60

Prepared for:
CLIENT NAME HERE

Prepared by:
US ProTech, Inc.

12/01/2015

Client Target: Windows Workstation IP: 27.0.0.1

Scanning Service: US ProScan

Scan Type	Description
Data Breach Risk Scan	Scans the computer to discover sensitive data, who has access to that data, and vulnerabilities that could lead to a breach or unauthorized access to privileged information. Provides the most comprehensive view of cyber risk for a computer and offers estimated cyber-liability compared to federal regulatory imposed fines averaged from recent cases throughout the United States.

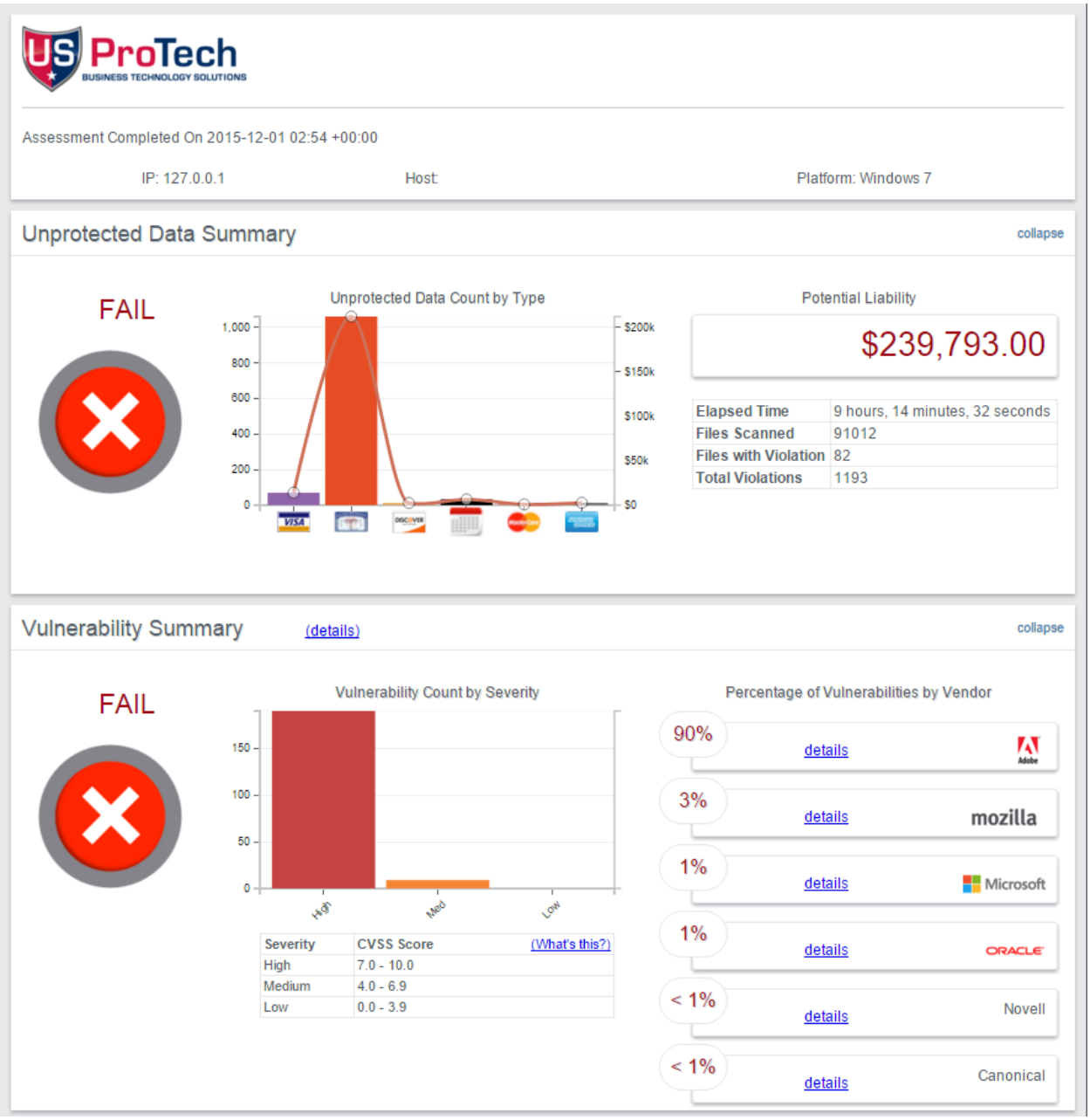
US ProScan is an internal cyber vulnerability and assessment scanner purpose built to identify known vulnerabilities, missing patches, misconfigurations, open ports and more. Integrated modules include:

PCI Compliance Scan (Internal)
Vulnerability and Patch scan for PCI requirement 11.2.1 plus 35 other PCI requirements that can be automated and audited with a scanner.

PAN Scan
Searches for non-compliant credit cardholder data across all your Windows and Mac OS X systems. Reports provide the location path of the credit card data along with the card brand type and number of targets such as drivers licenses numbers, DOB, etc.

BYOD Security Scanning
Cloud-based Security Scanning Service — US ProScan is an online security scanning service delivered from the cloud to Windows, Mac and Mobile devices. Opportunistically assess devices as they connect to your network and applications from anywhere in the world.

When deployed under a managed security service, US ProScan also has built-in features that include “locate, lock & wipe” features to assist in the protection of lost or stolen privileged data.



Enforcement and Penalties: (see: http://www.reyrey.com/regulations/) The dollar figure shown above is based upon national averages for fines imposed upon an entity in the event Personal Protected Information (PPI) data was accessed by unauthorized parties. The amount does not include the expenses associated to any remediation efforts or damages imposed by a court of law.

EXAMPLE / Oregon State: Security Breach
Any person that owns, maintains or otherwise possesses data that includes a consumers personal information that is used in the course of the persons business, vocation, occupation or volunteer activities and was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security, or receipt of notification to any consumer whose personal information was included in the information that was breached. Oregon.Rev.Stat. § 646.600 et seq

Social Security Statutes
A person shall not print a consumers SSN on any materials not requested by consumer or print the SSN on any card required to access products or services provided by the person or shall not publicly display or post or otherwise make available the SSN. Oregon.Rev.Stat. §646A.620

Notification
The disclosure notification shall be made in the most expeditious time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine sufficient contact information for the consumers, determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the data.

Notification is not required if, after an appropriate investigation or after consultation with law enforcement, the person determines that no reasonable likelihood of harm to the consumers whose personal information has been acquired has resulted or will result from the breach. Such a determination must be documented in writing and the documentation must be maintained for five years

Enforcement and Penalties
$1000 per violation, every violation is a separate offense and each days continuance a separate violation up to a maximum penalty of $500,000.

Unprotected Data Details | Edit Exclusion List | Download CSV data here | expand

Unprotected Data Scan Statistics | collapse

Elapsed Time	9 hours, 13 minutes, 32 seconds	
Volumes Scanned	Drive Root	D:\
	Drive Capacity	0
	Free Space	0
	Used Space	0
	Drive Root	F:\
	Drive Capacity	2,000,290,414,592
	Free Space	1,813,778,870,272
	Used Space	186,511,544,320
	Drive Root	C:\
	Drive Capacity	200,139,599,872
	Free Space	9,995,341,824
	Used Space	190,144,258,048
Files Scanned	91,012	
Files With Suspect Data	82	
Bytes Scanned	45,293,329,920	
Suspected Instances Found	1,193	

Vulnerability by Vendor Details | expand

Vulnerability Details

To further understand the CVSS Scoring system, see the National Vulnerability Database Calculator
The following section details the vulnerability's that were discovered during the scan. While this user has been applying the Microsoft updates and security patches, most of their applications have not been updated, which leaves this system vulnerable to attack.

Vulnerability Scan Details

Your system was scanned for vulnerabilities. At this time, no critical vulnerabilities were detected; however other Critical Patch Updates are currently available and are as follows:

Vulnerability Details Download CSV data here collapse

Windows 7 Vulnerability Policy Details

7367 - Buffer overflow vulnerability in Adobe Flash Player and Adobe AIR - XXII Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to buffer overflow vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code via unspecified vectors.

CVSS: 10.0

External Identifiers

CVE-2012-5250

15540 - Remote memory corruption vulnerability in Adobe Flash Player and Adobe Air - CVE-2013-3361 Vulnerable

The host is installed with Adobe Flash Player before 11.7.700.242 , 11.8.x before 11.8.800.168 or Adobe Air before 3.8.0.1430 and is prone to a remote memory corruption vulnerability. A flaw is present in the applications, which fail to handle crafted data. Successful exploitation could allow attackers to execute arbitrary code or crash the service.

CVSS: 10.0

External Identifiers

CVE-2013-3361

16552 - Security bypass vulnerability in Adobe Flash Player and Adobe AIR via unknown vectors - CVE-2014-0491 Vulnerable

The host is installed with Adobe Flash Player before 11.7.700.260, 11.8.x, 11.9.x before 12.0.0.38 or Adobe AIR before 4.0.0.1390 and is prone to security bypass vulnerability. The flaw is present in the applications, which fails to handle unknown vectors. Successful exploitation allows remote attackers to bypass unspecified protection mechanisms.

CVSS: 10.0

External Identifiers

CVE-2014-0491

10339 - Buffer overflow vulnerability in Adobe Flash Player and Adobe AIR via unspecified vectors - CVE-2013-1370 Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 or Adobe Air before 3.6.0.597 and is prone to a buffer overflow vulnerability. A flaw is present in the application, which fails to handle unspecified vectors. Successful exploitation could allow attackers to execute arbitrary code.

CVSS: 10.0

External Identifiers

CVE-2013-1370

7382 - Buffer overflow vulnerability in Adobe Flash Player and Adobe AIR - XXXII Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to buffer overflow vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code via unspecified vectors.

CVSS: 10.0

External Identifiers

CVE-2012-5265

7383 - Buffer overflow vulnerability in Adobe Flash Player and Adobe AIR - XXXIII Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to buffer overflow vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code via unspecified vectors.

CVSS: 10.0

External Identifiers

CVE-2012-5266

16792 - Memory corruption vulnerability in Adobe Shockwave Player - CVE-2014-0501 Vulnerable

The host is installed with Adobe Shockwave Player before 12.0.9.149 and is prone to memory corruption vulnerability. A flaw is present in the application, which fails to properly handle certain vectors related to memory. Successful exploitation allows attackers to cause a denial of service.

CVSS: 10.0

External Identifiers

CVE-2014-0501

7381 - Buffer overflow vulnerability in Adobe Flash Player and Adobe AIR - XXXI Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to buffer overflow vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code via unspecified vectors.

CVSS: 10.0

External Identifiers

CVE-2012-5264

7384 - Memory corruption vulnerability in Adobe Flash Player or Adobe AIR - XXXV Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to memory corruption vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code or cause a denial of service.

CVSS: 10.0

External Identifiers

CVE-2012-5267

7380 - Memory corruption vulnerability in Adobe Flash Player or Adobe AIR - XXIV Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to memory corruption vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code or cause a denial of service.

CVSS: 10.0

External Identifiers

CVE-2012-5263

7385 - Memory corruption vulnerability in Adobe Flash Player or Adobe AIR - XXIV Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to memory corruption vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code or cause a denial of service.

CVSS: 10.0

External Identifiers

CVE-2012-5268

4970 - Memory corruption vulnerability in Adobe Flash Player and Adobe AIR in the NetStream class Vulnerable

The host is installed with Adobe Flash Player 11.x before 11.2.202.228 or before 10.3.183.18 or Adobe AIR before 3.2.0.2070 and is prone to memory corruption vulnerability. A flaw is present in the applications, which fail to properly handle the NetStream class. Successful exploitation allows remote attackers to execute arbitrary code or cause a denial of service.

CVSS: 10.0

External Identifiers

CVE-2012-0773

10029 - Buffer overflow vulnerability in Adobe Flash Player and Adobe AIR - CVE-2013-2555 Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.75, 11.x before 11.7.700.169 or Adobe AIR before 3.7.0.1530 is prone to buffer overflow vulnerability. A flaw is present in the application(s), which fails to properly handle memory. Successful exploitation allow attackers to execute remote code or cause denial of service.

CVSS: 10.0

External Identifiers

CVE-2013-2555

16791 - Memory corruption vulnerability in Adobe Shockwave Player - CVE-2014-0500 Vulnerable

The host is installed with Adobe Shockwave Player before 12.0.9.149 and is prone to memory corruption vulnerability. A flaw is present in the application, which fails to properly handle certain vectors related to memory. Successful exploitation allows attackers to cause a denial of service.

CVSS: 10.0

External Identifiers

CVE-2014-0500

7386 - Memory corruption vulnerability in Adobe Flash Player or Adobe AIR - XXVII Vulnerable

The host is installed with Adobe Flash Player before 10.3.183.29 or 11.x before 11.4.402.287 or Adobe AIR 3.4.0.2540 or before and is prone to memory corruption vulnerability. A flaw is present in the applications, which fail to properly handle memory. Successful exploitation allows attackers to execute arbitrary code or cause a denial of service.

CVSS: 10.0

External Identifiers

CVE-2012-5269

Note: Over 50 Pages of finding have been removed to keep this SAMPLE Report under 10 pages

Conclusion:

The summary of the findings suggest that a substantial amount of effort would be required to effectively remove the identified sensitive data from the device. However, without an enforceable process and a written set of policies and procedures that would prevent the presence of this data being available in an unencrypted form, the likelihood of a reoccurrence would remain high.

US ProTech remains available and ready for any further professional support service regarding this matter and we suggest taking action to remedy any findings at the first opportunity of the IT Departments availability.

Sincerely,

The US ProTech Cyber-Security Team