`

Sample Vulnerability Assessment Report - Example Institute

Prepared By

sales@purplesec.us

Table of Contents

sales@purplesec.us

1. Executive Summary

The purpose of this vulnerability scan is to gather data on Windows and third-party software patch levels on specified hosts in the domain. The audit was performed on "DATE" using Nessus v8.2.2.

Of the 35 hosts identified, 32 systems were found to be active and were scanned. A total of 447 unique vulnerabilities were found during this scan. Critical, high, and medium severity vulnerabilities were found to exist across all 32 systems.

Vulnerability Risk	Unique Count
Critical Severity Vulnerabilities	44
High Severity Vulnerabilities	309
Medium Severity Vulnerabilities	84
Low Severity Vulnerabilities	10

The vulnerabilities found on Windows hosts consist of outdated Windows patches and third-party software including Google Chrome and Adobe Flash. Systems were also found to be missing patches from 2014. Older vulnerabilities present a more significant risk as malicious actors will often automate exploitation of known vulnerabilities in an attempt to catch the lowest hanging fruit. Therefore, we strongly recommend applying the latest patch to the outdated software as soon as possible.

The vulnerabilities found on the HP switches consist of TLS/SSL certificate vulnerabilities and deal mainly with using outdated encryption suites. Though outdated/self-signed certificates on internal devices are not as high risk as the same on external facing devices, proper, up-to-date SSL certificates should be installed to meet best practice. Additionally, switches were found to be running variations of 3 versions of firmware; these switches should be updated to the newest firmware supported by the vendor.

It is our recommendation that immediate action be taken to resolve these vulnerabilities by applying patches and adjusting system configurations as necessary.

In addition, a patch and configuration management process should be implemented to continually assess system risk level as vulnerabilities are discovered. This will ensure relevant security patches and configurations are applied in a timely manner.

2. Scan Results

We have included supplemental material to this report consisting of the Nessus scan results and Nessus report.

Scan Results - The scan results provide granular detail of each vulnerability, which are categorized by their severity: critical, high, medium, and low. An expanded definition of the known threat and solutions for remediating the vulnerability are also available.

Nessus Report – The Nessus Report provides a comprehensive analysis of the scan results.

sales@purplesec.us

3. Methodology

Internal credentialed patch audits are used as a tool to gather data in order to assess the effectiveness of "the client patching effort. Further, this data will be used to support findings and recommendations found under the "Recommendations" section.

The scan was conducted using the Nessus Professional vulnerability scanning platform connected to the "THE CLIENT" environment. The purpose of utilizing a scanning engine inside the network perimeter along with valid domain credentials is to bypass existing external security controls and host-based security measures to gain a detailed look at system configuration and patch levels. The 00.00.00.0/00 subnet was identified by "THE CLIENT", with further specification to scan hosts residing in the "THE CLIENT" domain.

When performing vulnerability scans, the risk of system crash or degraded performance is always present. In order to mitigate risk of system downtime or impairment, some systems (such as network switches or printers) are excluded from scans.

The vulnerability scan occurs in two phases:

1. Network Discovery
2. Vulnerability Assessment

The network discovery phase is conducted to discover live hosts on the target network and involves various host discovery methods such as ICMP pings, ARP pings, and TCP connections to well-known ports. The vulnerability assessment uses data gathered during the first phase to generate the report.

4. Findings

The results from the credentialed patch audit are listed below. It is important to note that not all identified hosts were able to be scanned during this assessment – of the 35 hosts identified by "THE CLIENT" as belonging to the "THE CLIENT" domain, only 32 were successfully scanned. In addition, some of the hosts scanned were not included in the host list provided.

The remainder of the hosts were either offline during scans or the supplied credentials failed to authenticate to the hosts. Though not all hosts were not able to be scanned, the findings should be representative of the current overall vulnerability status of hosts in the network.

A full listing of scanned hosts is available in the "Scan Results" section of this report.

- Outdated Windows Patch Levels: Many systems reported the need for patches and updates that have been published for at least thirty-days.
- Outdated Third-Party Software: Many systems reported missing necessary security updates for popular third-party software packages such Google Chrome, and Adobe Flash.

sales@purplesec.us

5. Risk Assessment

This report identifies security risks that could have significant impact on mission-critical applications used in day-to-day business operations. These risks are quantified according to their likelihood of occurrence and the potential damage if they occur. Risk factors are combined to form an overall risk index for each system, allowing you to prioritize your remediation activities accordingly. Of the 32 systems scanned, a total of 447 unique vulnerabilities were found.

Vulnerability Risk	Unique Count
Critical Severity Vulnerabilities	44
High Severity Vulnerabilities	309
Medium Severity Vulnerabilities	84
Low Severity Vulnerabilities	10

Critical Severity Vulnerability

44 were critical severity vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems.

A list of the most frequent critical severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
KB4022715: Windows 10 Version 1607 and Windows Server 2016 June 2017 Cumulative Update	The remote Windows host is missing security update KB4022715. It is therefore affected by multiple vulnerabilities. A local attacker can exploit these via a specially crafted script to bypass the Device Guard Code Integrity policy and inject arbitrary code into a trusted PowerShell process.	Apply security update KB4022715 as well as refer to the KB article for additional information.	5
Security Updates for Microsoft .NET Framework (February 2019)	The Microsoft .NET Framework installation on the remote host is missing security updates. A remote code execution vulnerability exists in .NET Framework and Visual Studio software when the software fails to check the source markup of a file. An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user.	Microsoft has released security updates for Microsoft .NET Framework.	4
Security Updates for Microsoft .NET Framework (December 2018)	The Microsoft .NET Framework installation on the remote host is missing security updates. A remote code execution vulnerability exists when the Microsoft .NET Framework fails to validate input properly. An attacker who successfully exploited this vulnerability could take control of an affected system. An attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.	Microsoft has released security updates for Microsoft .NET Framework.	4

sales@purplesec.us

Microsoft SQL Server Unsupported Version Detection	According to its self-reported version number, the installation of Microsoft SQL Server on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.	Upgrade to a version of Microsoft SQL Server that is currently supported.	3
MS16-077: Security Update for WPAD (3165191)	The remote Windows host is missing a security update. An elevation of privilege vulnerability exists in the Web Proxy Auto Discovery (WPAD) protocol due to improper handling of the proxy discovery process. A remote attacker can exploit this by responding to NetBIOS name requests for WPAD to bypass security restrictions and gain elevated privileges.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, RT 8.1, 2012 R2, and 10. Note that cumulative update 3160005 in MS16-063 must also be installed in order to fully resolve CVE-2016-3213.	3

High Severity Vulnerability

309 were high severity vulnerabilities. High severity vulnerabilities are often harder to exploit and may not provide the same access to affected systems.

A list of the most frequent high severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
MS15-011: Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)	The remote Windows host is affected by a remote code execution vulnerability due to how the Group Policy service manages policy data when a domain-joined system connects to a domain controller. An attacker using a controlled network can exploit this to gain complete control of the host. Note that Microsoft has no plans to release an update for Windows 2003 even though it is affected by this vulnerability.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.	18
Security Updates for Internet Explorer (June 2017)	The Internet Explorer installation on the remote host is missing security updates. A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory. This vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user	Microsoft has released security updates for the affected versions of Internet Explorer.	18

MS15-124: Cumulative Security Update for Internet Explorer (3116180)	The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3116180. An unauthenticated remote attacker can exploit these issues by convincing a user to visit a specially crafted website resulting in the execution of arbitrary code in the context of the current user.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT, 2012, 8.1, RT 8.1, 2012 R2, and 10.	18
KB4056898: Windows 8.1 and Windows Server 2012 R2 January 2018 Security Update (Meltdown)(Spectre)	The remote Windows host is missing security update 4056898 or cumulative update 4056895. A vulnerability exists within microprocessors utilizing speculative execution and indirect branch prediction which may allow an attacker with local user access to disclose information via a side-channel analysis	Apply Security Only update KB4056898 or Cumulative Update KB4056895. Due to a compatibility issue with some antivirus software products it may not be possible to apply the required updates.	9
KB4343888: Windows 8.1 and Windows Server 2012 R2 August 2018 Security Update (Foreshadow)	The remote Windows host is missing security update 4343888 or cumulative update 4343898. A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory. The vulnerability could corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user	Apply Security Only update KB4343888 or Cumulative Update KB4343898 as well as refer to the KB article for additional information.	9

sales@purplesec.us

Medium Severity Vulnerability

84 were medium severity vulnerabilities. These vulnerabilities often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner but are not as urgent as the other vulnerabilities.

A list of the most frequent medium severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected.	Force the use of SSL as a transport layer for this service if supported| or/and - Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.	19
MS KB3009008: Vulnerability in SSL 3.0 Could Allow Information Disclosure (POODLE)	The remote host is missing one of the workarounds referenced in the Microsoft Security Advisory 3009008. If the client registry key workaround has not been applied, any client software installed on the remote host (including IE) is affected by an information disclosure vulnerability when using SSL 3.0.	Apply the client registry key workaround and the server registry key workaround suggested by Microsoft in the advisory.	18
Microsoft Windows Unquoted Service Path Enumeration	The remote Windows host has at least one service installed that uses an unquoted service path, which contains at least one whitespace. A local attacker can gain elevated privileges by inserting an executable file in the path of the affected service	Ensure that any services that contain a space in the path enclose the path in quotes.	7
Security Updates for Microsoft .NET Framework (January 2019)	The Microsoft .NET Framework installation on the remote host is missing a security update. An attacker who successfully exploited the vulnerability could retrieve content, that is normally restricted, from a web application.	Microsoft has released security updates for Microsoft .NET Framework.	4

ADV180002: Microsoft SQL Server January 2018 Security Update (Meltdown) (Spectre)	The remote Microsoft SQL Server is missing a security update. It is, therefore, affected by a vulnerability exists within microprocessors utilizing speculative execution and indirect branch prediction, which may allow an attacker with local user access to disclose information via a side-channel analysis.	Microsoft has released a set of patches for SQL Server 2008, 2008 R2, 2012, 2014, 2016, and 2017.	4

Low Severity Vulnerability

10 were low severity vulnerabilities. Low severity vulnerabilities do not need to be patch immediately and can be resolved during the next updates maintenance window.

A list of the most frequent critical severity vulnerabilities is provided below:

PLUGIN NAME	DESCRIPTION	SOLUTION	COUNT
MS16-153: Security Update for Common Log File System Driver (3207328)	The remote Windows host is missing a security update. It is, therefore, affected by an information disclosure vulnerability in the Windows Common Log File System (CLFS) due to improper handling of objects in memory. A local attacker can exploit this vulnerability, via a specially crafted application, to bypass security measures and disclose sensitive information.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016.	2
MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (3004365)	The remote Windows host is affected by a vulnerability in the Windows Error Reporting service component that allows bypassing the 'Protected Process Light' security feature. A remote attacker can exploit this vulnerability to gain access to the memory of a running process.	Microsoft has released a set of patches for Windows 8, 2012, 8.1, and 2012 R2.	1
MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass (3004361)	The version of Windows running on the remote host is affected by a security downgrade vulnerability that affects workstations and servers configured to use Group Policy. A man-in-the-middle attacker can cause the policy file to become corrupted and unreadable, resulting in the Group Policy settings reverting to their default, potentially less secure state.	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.	1

sales@purplesec.us

Microsoft Exchange Server Elevation of Privilege Vulnerability (November 2018)	The Microsoft Exchange install on the remote host contains an unspecified flaw that allows an authenticated man-in-the-middle attacker to impersonate another user and escalate privileges.	Delete the following registry value: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\DisableLoopbackCheck as shown in the advisory.	1
MS16-124: Security Update for Windows Registry (3193227)	The remote Windows host is missing a security update. It is, therefore, affected by multiple information disclosure vulnerabilities in the kernel API that allow a local attacker, via a specially crafted application, to disclose sensitive registry information.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.	1

6. Recommendations

Recommendations in this report are based on the available findings from the credentialed patch audit. Vulnerability scanning is only one tool to assess the security posture of a network. The results should not be interpreted as definitive measurement of the security posture of the "THE CLIENT" network. Other elements used to assess the current security posture would include policy review, a review of internal security controls and procedures, or internal red teaming/penetration testing.

Patch management and system configuration are the main security elements that need to be addressed by "THE CLIENT". While it is possible to remediate all discovered vulnerabilities through applying patches or adjusting system configurations, issues will re-appear as new vulnerabilities are discovered.

It is recommended that a patch and configuration management process be implemented to audit system risk level and configuration drift on a regular basis to ensure that relevant security patches and configuration changes are applied in a timely manner.

sales@purplesec.us

Remediation

Taking the following actions across 9 hosts will resolve 20% of the vulnerabilities on the network:

ACTION TO TAKE	VULNS	HOSTS
Adobe Flash Player <= 32.0.0.114 (APSB19-06): Upgrade to Adobe Flash Player version 32.0.0.142 or later	767	1
MS KB3065823: Update for Vulnerabilities in Adobe Flash Player in Internet Explorer: Install Microsoft KB3065823.	172	1
Install KB4489873	135	5
Install KB4489881	72	1
Install KB4489891	47	1
Google Chrome < 73.0.3683.75 Multiple Vulnerabilities: Upgrade to Google Chrome version 73.0.3683.75 or later.	18	1
Install KB4489880	16	1
Microsoft Malware Protection Engine < 1.1.14700.5 RCE: Enable automatic updates to update the scan engine for the relevant antimalware applications. Refer to Knowledge Base Article 2510781 for information on how to verify that MMPE has been updated.	11	1
HP Insight Management Agents Multiple Vulnerabilities: Upgrade to HP Insight Management Agents 9.0.0.0 or later.	8	2
Install KB4489878	6	2
Install KB4023307	6	2
KB4023307: Security Update for the Windows Uniscribe Remote Code Execution Vulnerability for Microsoft Silverlight 5 (June 2017): Apply security update KB4023307.	6	2
Install MS18-01	5	1
Install KB3185911	5	1
Install KB4480059	4	1

Install KB4035055	4	1
Install KB4489882	4	2
Install KB4480058	3	1
Install KB4018466	3	1
Install KB4015380	3	1
Install KB4483453	3	1
Install KB3156019	3	1
Install KB3110329	3	1
Install KB2993651	3	1
Security Updates for Exchange (Jun 2018): Microsoft has released the following security updates to address this issue: -KB4295699 -KB4099855 -KB4099852	3	1
Install MS18-05	2	1
Install KB4457037	2	1
Install KB4483457	2	1
Install KB4470637	2	1
Install KB4457038	2	1
Install KB4344151	2	1
Install KB4344149	2	1

sales@purplesec.us

Install KB4340583	2	1
Install KB4039266	2	1
Install KB4026059	2	1
Install KB4025240	2	1
Install KB4015068	2	1
Install KB4012583	2	1
Install KB3170455	2	1
Install KB3157569	2	1
Install KB3126446	2	1
Install KB3133043	2	2
Install KB3126587	2	2
Install KB2538243	1	1
Install KB3135995	1	1
Install KB4489876	1	1
Install KB4093223	1	1
Install KB4048970	1	1
Install KB4025674	1	1

sales@purplesec.us

Install KB4022750	1	1
Install KB4018821	1	1
Install KB4015383	1	1
Install KB4014793	1	1
Install KB4014652	1	1
Install KB3216775	1	1
Install KB3197655	1	1
Install KB3196726	1	1
Install KB3196718	1	1
Install KB3188726	1	1
Install KB4480057	1	1
Install KB3184943	1	1
Install KB3156017	1	1
Install KB3153704	1	1
Install KB3135994	1	1
Install KB3109560	1	1
Install KB3097997	1	1

Install KB3084135	1	1
Install KB3076895	1	1
Install KB3075220	1	1
Install KB3004365	1	1
Install KB3000483	1	1
Install KB2957189	1	1
HP Version Control Agent (VCA) < 7.3.3 Multiple SSL Vulnerabilities: Upgrade to VCA 7.3.3 or later.	0	2

sales@purplesec.us

Security Policy & Configuration

All services users authenticate against, such as an internal Active Directory environment or a third-party provider of a CMS application, include some kind of security policy. Typically, this includes criteria around passwords, administrative access, and auditing.

Industry Best Practice

User accounts with administrative rights should be periodically reviewed and adjusted as necessary to comply with the principle of least privilege, which states that accounts have only the level of access necessary to perform required functions. If an account is compromised, the potential damage is therefore limited to the minimum amount possible.

Additionally, the following password and lockout settings are recommended:

Policy Setting	Description	Recommendation
Enforce Password History	The number of previous passwords that the user is prohibited from re-using.	24
Maximum Password Age	The maximum length of time that may elapse before a user is forced to change their password	120 Days
Minimum Password Age	The length of time that must pass before a user can change their password again	1 Day
Minimum Password Length	The number of characters that must be used in a password	8 Characters
Password Complexity Requirements	Requires users to use 2 out of 3 of Upper Case, Number or Symbol in a password. E.g Pass2017, or test123!.	Enabled
Screen Lock Policy	Locks users workstation after specified duration of inactivity	15 Minutes or less
Account Lockout Policy	Disables access to an account for a specified duration after a number of login attempts with an invalid password. Is effective against automated attempts to guess user passwords.	30 Minute Lockout after 10 attempts