To: Jeremy Holck[jeremy.holck@dominionvoting.com]
From: Eric Coomer
Sent: Tue 9/29/2020 4:52:48 PM
Subject: Re: test
ATT86561.jpg
ATT54464.jpg
ATT33657.jpg
ATT07277.jpg

Coolio, I'll test after my meeting

ERIC D. COOMER | DIRECTOR, PRODUCT STRATEGY AND SECURITY

DOMINION VOTING
1201 18th Street, Suite 210, DENVER, CO 80202
1.866.654.8683 | DOMINIONVOTING.COM

720.201.1728MOBILE

From: Jeremy Holck <jeremy.holck@dominionvoting.com>
Sent: Tuesday, September 29, 2020 10:51:31 AM
To: Eric Coomer <eric.coomer@dominionvoting.com>
Subject: RE: test

I think it's a local caching issue, try this (screenshots below for reference):

- Compose a new message, delete the Security entry that is cached in the From list
- Click Other Email Address, click on the From field
- Change the dropdown under Address Book from the Offline Address List to the Global Address List and choose the Security Distribution Group, Click ok, ok

You and me have the same permissions so that should do it, if not, back to the drawing board

---

From: Eric Coomer <eric.coomer@dominionvoting.com>
Sent: Tuesday, September 29, 2020 10:40 AM
To: Jeremy Holck <jeremy.holck@dominionvoting.com>
Subject: FW: test

Still a no for me

ERIC D. COOMER | DIRECTOR, PRODUCT STRATEGY AND SECURITY

DOMINION VOTING
1201 18th Street, Suite 210, DENVER, CO 80202
1.866.654.8683 | DOMINIONVOTING.COM

720.201.1728 MOBILE

From: System Administrator
Sent: Tuesday, September 29, 2020 10:40 AM
Subject: Undeliverable: test

Your message did not reach some or all of the intended recipients.

Subject: test
Sent: 9/29/2020 10:40 AM

The following recipient(s) cannot be reached:

Eric Coomer on 9/29/2020 10:40 AM
This message could not be sent. You do not have the permission to send the message on behalf of the specified user.

Diagnostic information for administrators:

Error is [0x80070005-0x000004dc-0x00000524].

Exchange response headers:
request-id: d71c3e1e-c6d0-4ac6-bd77-0c317958df16
X-ServerApplication: Exchange/15.20.3412.030
X-FEServer: CO2PR04CA0190
X-BEServer: CY4PR1301MB2168
X-CalculatedBETarget: CY4PR1301MB2168.NAMPRD13.PROD.OUTLOOK.COM
X-RequestId: {C538D1AE-3D8B-4BC4-A3B1-CB3AF32B7A02}:280
X-ClientInfo: {15AD8E19-1458-49AC-9719-AC1C5CEA2161}:116360030
X-ElapsedTime: 124
X-BackEndHttpStatus: 200
X-ResponseCode: 0
X-DiagInfo: CY4PR1301MB2168
X-RequestType: Execute

ROPs Summary:

0: ropSetProps (10) Processed(1) Completed(0)
ROP result: 0
Response codes: 0
1: ropSetProps (10) Processed(1) Completed(0)

```
                ROP result: 0
                Response codes: 0
        2: ropSetProps (10) Processed(1) Completed(0)
                ROP result: 0
                Response codes: 0
        3: ropFlushRecipients (14) Processed(1) Completed(0)
                ROP result: 0
                Response codes: 0
        4: ropSetProps (10) Processed(1) Completed(0)
                ROP result: 0
                Response codes: 0
        5: ropTransportSend (74) Processed(1) Completed(0)
                ROP result: 0
                Response codes: 1244
```

```
Response Exceptions:

ROP Index: 5
ROP Associated: ropTransportSend (74)
Microsoft.Exchange.Data.Storage.SendAsDeniedException: Can't transport send
message. ---> Microsoft.Mapi.MapiExceptionSendAsDenied:
MapiExceptionSendAsDenied: Unable to transport send message. (hr=0x80070005,
ec=1244)
Diagnostic context:
    Lid: 35250
    Lid: 36674   dwParam: 0x1
    Lid: 61250   dwParam: 0x0
    Lid: 45378   dwParam: 0x2
    Lid: 44866   dwParam: 0x0
    Lid: 36674   dwParam: 0x1
    Lid: 61250   dwParam: 0x0
    Lid: 45378   dwParam: 0x5
    Lid: 44866   dwParam: 0x0
    Lid: 36674   dwParam: 0x7A
    Lid: 61250   dwParam: 0x0
    Lid: 45378   dwParam: 0x8
    Lid: 44866   dwParam: 0x1400
    Lid: 36674   dwParam: 0xA
    Lid: 61250   dwParam: 0x0
    Lid: 45378   dwParam: 0x19
    Lid: 44866   dwParam: 0x13C7
    Lid: 36674   dwParam: 0xE
    Lid: 61250   dwParam: 0x0
    Lid: 45378   dwParam: 0x13E3
    Lid: 44866   dwParam: 0x24A
    Lid: 55847   EMSMDBPOOL.EcPoolSessionDoRpc called [length=3389]
    Lid: 43559   EMSMDBPOOL.EcPoolSessionDoRpc returned
[ec=0x0][length=164][latency=2]
    Lid: 52176   ClientVersion: 15.20.3412.30
    Lid: 50032   ServerVersion: 15.20.3412.6030
    Lid: 35180
```

```
    Lid: 23226   --- ROP Parse Start ---
    Lid: 27962   ROP: ropDeletePropsNoReplicate [122]
    Lid: 27962   ROP: ropSetProps [10]
    Lid: 27962   ROP: ropFlushRecipients [14]
    Lid: 31418   --- ROP Parse Done ---
    Lid: 35250
    Lid: 36674   dwParam: 0xA
    Lid: 61250   dwParam: 0x0
    Lid: 45378   dwParam: 0x2
    Lid: 44866   dwParam: 0x18
    Lid: 36674   dwParam: 0x4A
    Lid: 61250   dwParam: 0x0
    Lid: 45378   dwParam: 0x1D
    Lid: 44866   dwParam: 0x0
    Lid: 55847   EMSMDBPOOL.EcPoolSessionDoRpc called [length=126]
    Lid: 43559   EMSMDBPOOL.EcPoolSessionDoRpc returned
[ec=0x0][length=464][latency=0]
    Lid: 52176   ClientVersion: 15.20.3412.30
    Lid: 50032   ServerVersion: 15.20.3412.6030
    Lid: 35180
    Lid: 23226   --- ROP Parse Start ---
    Lid: 27962   ROP: ropSetProps [10]
    Lid: 27962   ROP: ropTransportSend [74]
    Lid: 17082   ROP Error: 0x4DC
    Lid: 44949
    Lid: 21921   StoreEc: 0x4DC
    Lid: 27962   ROP: ropExtendedError [250]
    Lid: 1494    ---- Remote Context Beg ----
    Lid: 38698
    Lid: 37692
    Lid: 37948
    Lid: 33852   dwParam: 0x0        Msg: SMTP
    Lid: 56248   StoreEc: 0x4DC
    Lid: 40748   qdwParam: 0x74D7384200000001
    Lid: 57132   qdwParam: 0x0
    Lid: 63016   dwParam: 0x4A
    Lid: 39640   StoreEc: 0x4DC
    Lid: 45434   Guid: 112d8e51-0f77-4e55-9fb2-bb46aaaf5206
    Lid: 10786   dwParam: 0x0        Msg:
15.20.3412.030:CY4PR1301MB2168:76e869ad-9072-41d5-9852-8245674b138b
    Lid: 51330   qdwParam: 0x8D864964076FD6B
    Lid: 39570
    Lid: 55954   dwParam: 0xA
    Lid: 49266
    Lid: 33010   dwParam: 0xA
    Lid: 54258   Error: 0x0
    Lid: 40002
    Lid: 56562   dwParam: 0x0
    Lid: 64146   dwParam: 0x4A
    Lid: 33010   dwParam: 0x4A
    Lid: 54258   Error: 0x4DC
    Lid: 1750    ---- Remote Context End ----
```

```
    Lid: 31418   --- ROP Parse Done ---
    Lid: 22753
    Lid: 21817   ROP Failure: 0x4DC
    Lid: 34722
    Lid: 51106   StoreEc: 0x4DC
    Lid: 41890
    Lid: 58274   StoreEc: 0x4DC
    Lid: 59285
    Lid: 46997   StoreEc: 0x4DC
   at Microsoft.Mapi.MapiExceptionHelper.InternalThrowIfErrorOrWarning(String
message, Int32 hresult, Boolean allowWarnings, Int32 ec, DiagnosticContext
diagCtx, Exception innerException, MapiStore mapiStore)
   at Microsoft.Mapi.MapiExceptionHelper.ThrowIfError(String message, Int32
hresult, IExInterface iUnknown, Exception innerException, MapiStore mapiStore)
   at Microsoft.Mapi.MapiBase.ThrowIfError(String message, Int32 hr)
   at Microsoft.Mapi.MapiMessage.TransportSendMessage(PropValue[]&
propsToReturn)
   at Microsoft.Exchange.Data.Storage.MapiAccessor.TransportSendMessage(Object
mapiObject, ExTimeZone timezone, PropValue[]& mapiPropValues)
   --- End of inner exception stack trace ---
   at Microsoft.Exchange.Data.Storage.MapiAccessor.TransportSendMessage(Object
mapiObject, ExTimeZone timezone,


Transport-Send failed: failure enum(25), HResult(0x00000000), EC(1244).
Transport-Send failed: failure enum(22), HResult(0x00000000), EC(1244).
Submit-Message failed: message id(20), failure enum(13), HResult(0x80070005),
EC(1244).
```

To: Jeremy Holck[jeremy.holck@dominionvoting.com]; Andrew Hall[andrew@hallstarsolutions.com]
Cc: Mike McGee[michael.mcgee@dominionvoting.com]; Paul MacLaren (rockfishmarketing@bell.net)[rockfishmarketing@bell.net]; Paul MacLaren (rockfishmarketing@bell.net)[rockfishmarketing@bell.net]
From: Eric Coomer
Sent: Thur 10/1/2020 7:40:55 PM
Subject: Re: [EXTERNAL] Bug Report

Thanks Andrew, can you provide a brief description of the mitigation taken to address?

ERIC D. COOMER | DIRECTOR, PRODUCT STRATEGY AND SECURITY

DOMINION VOTING
1201 18th Street, Suite 210, DENVER, CO 80202
1.866.654.8683 | DOMINIONVOTING.COM

720.201.1728MOBILE

From: Andrew Hall <andrew@hallstarsolutions.com>
Sent: Thursday, October 1, 2020 12:54:38 PM
To: Jeremy Holck <jeremy.holck@dominionvoting.com>
Cc: Eric Coomer <eric.coomer@dominionvoting.com>; Mike McGee <michael.mcgee@dominionvoting.com>; Paul MacLaren (rockfishmarketing@bell.net) <rockfishmarketing@bell.net>; Paul MacLaren (rockfishmarketing@bell.net) <rockfishmarketing@bell.net>
Subject: RE: [EXTERNAL] Bug Report

Jeremy et al,

The vulnerability described below has been eliminated.

Regards,

Andrew JK Hall
Digital Portfolio Director / Owner
M: 905-599-3448 | andrew@hallstarsolutions.com | www.hallstarsolutions.com | www.linkedin.com/in/ahallstar

1100 Burloak Drive, Suite 300 | Burlington, Ontario | L7L 6B2

advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please reply blank email and delete it immediately.

From: Jeremy Holck <jeremy.holck@dominionvoting.com>
Sent: Thursday, October 1, 2020 12:26 PM
To: Andrew Hall <andrew@hallstarsolutions.com>
Cc: Eric Coomer <eric.coomer@dominionvoting.com>; Mike McGee <michael.mcgee@dominionvoting.com>; Paul MacLaren (rockfishmarketing@bell.net) <rockfishmarketing@bell.net>
Subject: RE: [EXTERNAL] Bug Report

There wasn't any additional text. From a proof of concept view, the commands listed in step C and the attached screenshot show the impact.

From: Andrew Hall <andrew@hallstarsolutions.com>
Sent: Thursday, October 1, 2020 10:19 AM
To: Jeremy Holck <jeremy.holck@dominionvoting.com>
Cc: Eric Coomer <eric.coomer@dominionvoting.com>; Mike McGee <michael.mcgee@dominionvoting.com>; Paul MacLaren (rockfishmarketing@bell.net) <rockfishmarketing@bell.net>
Subject: RE: [EXTERNAL] Bug Report

Under "Proof of concept" is a blank space. Was there more to this message?

Regards,

Andrew JK Hall

Digital Portfolio Director / Owner

M: 905-599-3448 | andrew@hallstarsolutions.com | www.hallstarsolutions.com | www.linkedin.com/in/ahallstar

1100 Burloak Drive, Suite 300 | Burlington, Ontario | L7L 6B2

From: Jeremy Holck <jeremy.holck@dominionvoting.com>
Sent: Thursday, October 1, 2020 12:10 PM
To: Andrew Hall <andrew@hallstarsolutions.com>
Cc: Eric Coomer <eric.coomer@dominionvoting.com>; Mike McGee

<michael.mcgee@dominionvoting.com>
Subject: FW: [EXTERNAL] Bug Report

Andrew, we received a new vulnerability submission.

From: Mohd Asif Khan <blackops.asif@gmail.com>
Sent: Wednesday, September 30, 2020 11:50 PM
To: Security <Security@dominionvoting.com>
Subject: [EXTERNAL] Bug Report

Hello Security Team,
My name is Mohd Asif Khan and I am a Security Researcher.
I have found a bug in your site. Report of the bug is as follows:-

a) Summary:-
It's possible to get information about the users registered (such as: id, name, login name, etc.) without authentication in Wordpress via API on https://www.dominionvoting.com/wp-json/wp/v2/users

b) Description:-
By default Wordpress allows public access to the Rest API to get information about all users registered on the system.

c) Steps To Reproduce:-
1. Visit url:- https://www.dominionvoting.com/ and add /wp-json/wp/v2/users/
2. https://www.dominionvoting.com/wp-json/wp/v2/users
3. Add numbers like https://www.dominionvoting.com/wp-json/wp/v2/users (1,2,3,4....) to get information about the users.

d) Remediation:-
There are 2 ways that it's possible to fix this problem.
FIX 1 - It's possible to remove this access for anyone by changing the source code where when someone requests the Rest API and the server sends a 404 (Not Found) message for the user who made the request.
Reference: https://github.com/WP-API/WP-API/issues/2338

FIX 2 - It's also possible to create a rewrite rule on .htaccess (if the webserver it's Apache) to redirect any request that contain rest_route (eg.: "^.rest_route=/wp/") to a Not Found (404) or a Default Page.

e) Impact:-
It's possible to get all the users registered on the system and create a brute force directed to these users.

Reference:
https://hackerone.com/reports/356047

https://hackerone.com/reports/335779

f) Proof Of Concept:-