Microsoft

MSRC BLUEHAT OCT '23

"It's by-design"

Dr Nestori Syynimaa
@DrAzureAD

People of Microsoft,
I come in peace*!

* Nov 2023 edition

“It’s by-design”

- Vocabulary
- Cases

Vocabulary 1/3

Bug Bounty

“a reward offered to a person who identifies an error or ***vulnerability*** *in a computer program or system”* – Oxford dictionary

Security Vulnerability

"a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to ***confidentiality****,* ***integrity****,* OR ***availability****."*
– MITRE.org

Vocabulary 2/3

Bug Bounty Program

Bounties related to certain products or services, e.g., *Microsoft Azure* and *Microsoft Identity*

Out-of-scope

A vulnerability that doesn't fit into any Bug Bounty Program

By-design

"Something" that is not considered a vulnerability

Vocabulary 3/3

Severity

Four level categorization (Low, Moderate, Important, and Critical)

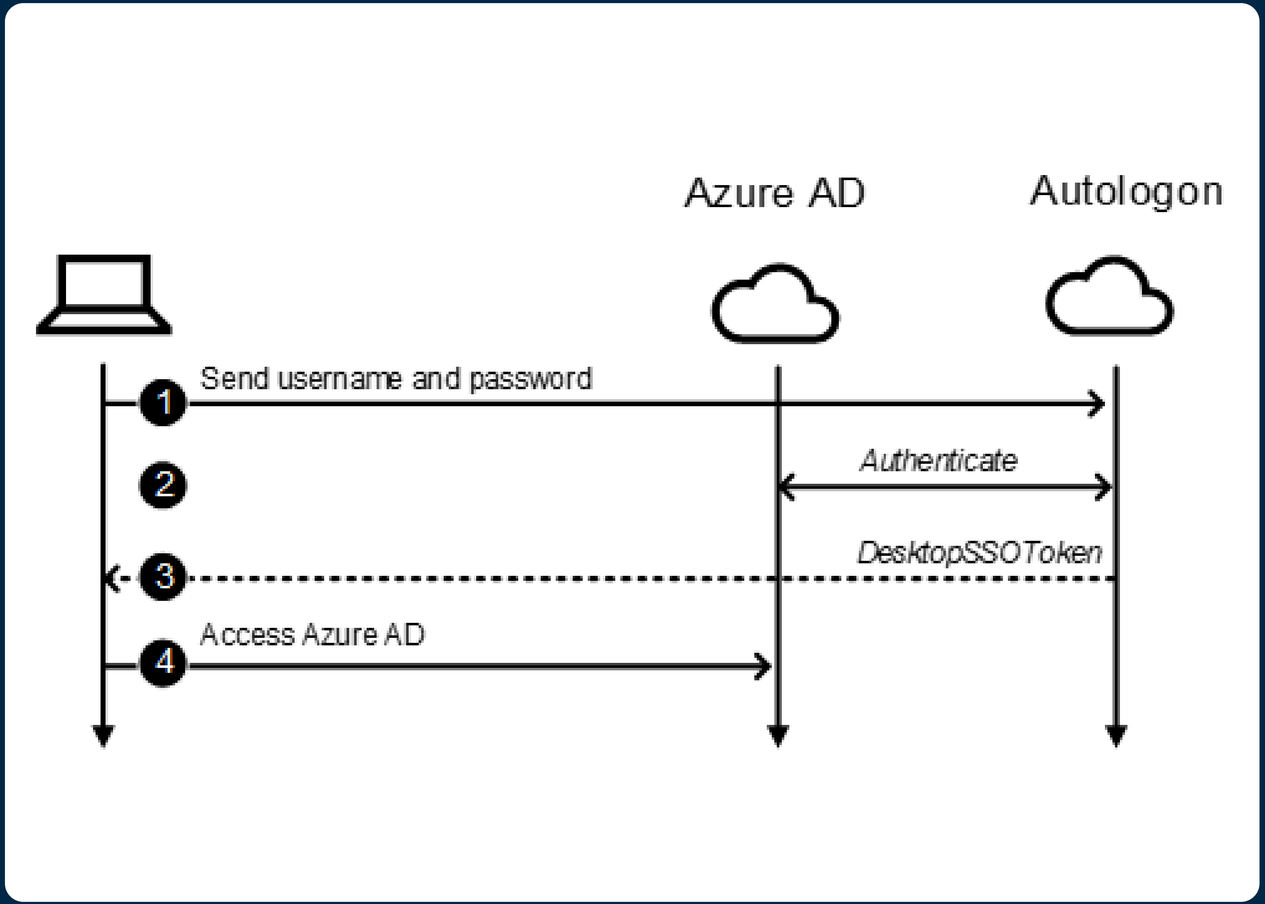
Microsoft typically offers bounties only for *Critical* and *Important*

Brute-forcing and user enumeration

Jun 2021 – Dec 2021

User enumeration & brute forcing using *autologon* endpoint

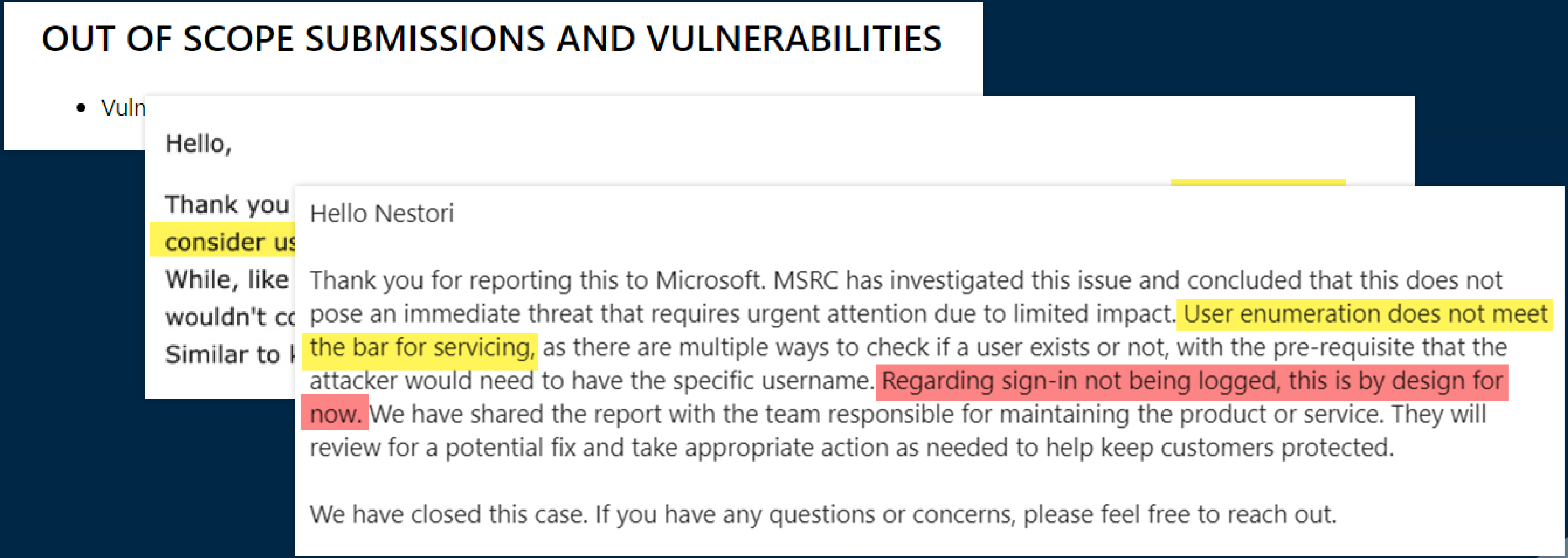
- Endpoint for Seamless Single-Sign-On (aka DesktopSSO)
  - Exchanges Kerberos Service Tickets to *DesktopSSOToken*
  - Supports also username and passwords (credits to @JoosuaSantasalo)



MITRE ATT&CK

- Reconnaissance (TA0043)
  - Gather Victim Identity Information (T1589)
  - .002 Email Addresses
  - .003 Employee Names
- Credential Access (TA0006)
  - Brute Force (T1110)

Response



OUT OF SCOPE SUBMISSIONS AND VULNERABILITIES

- Vuln

Hello,

Thank you
consider us
While, like
wouldn't co
Similar to k

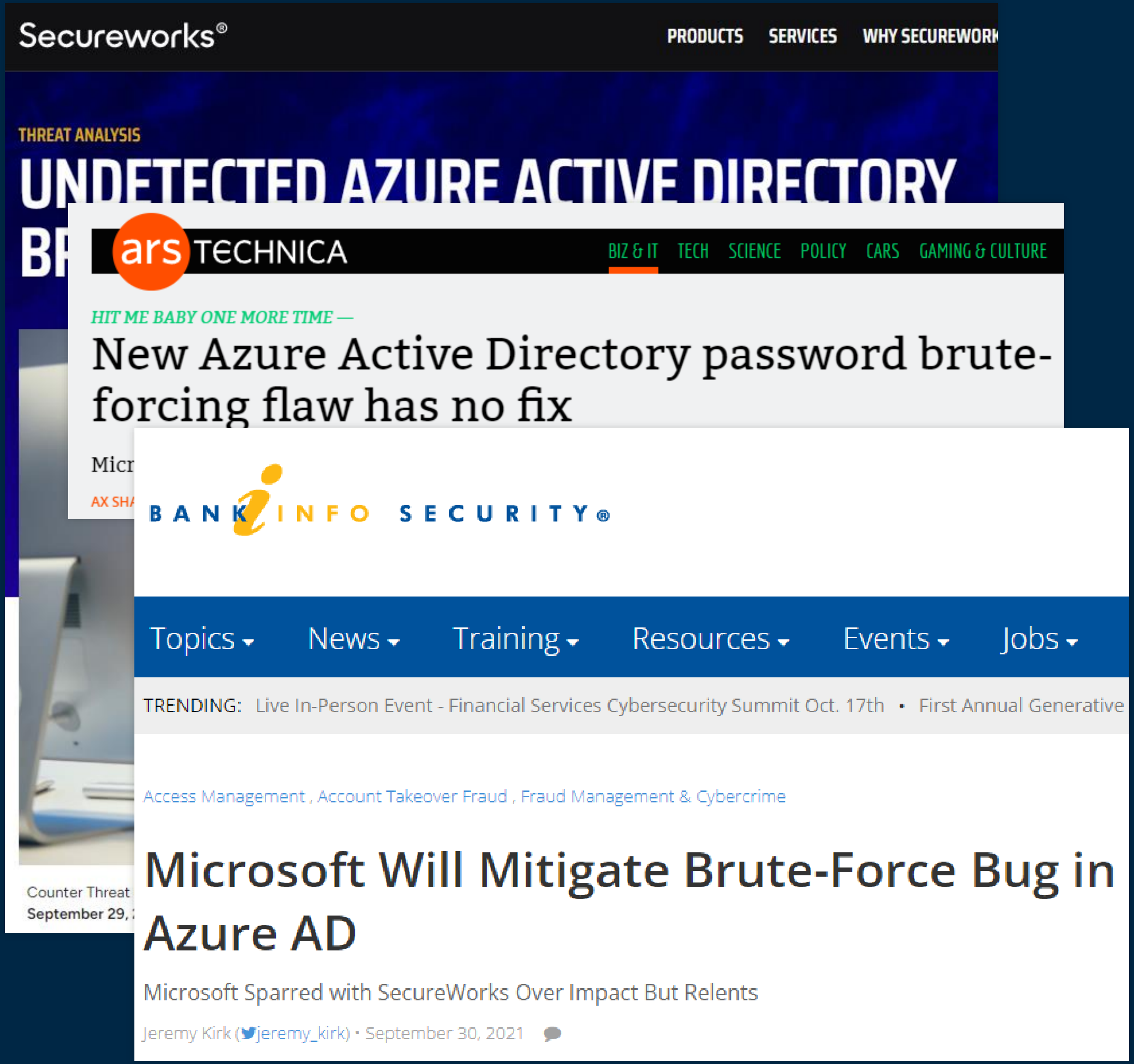
Hello Nestori

Thank you for reporting this to Microsoft. MSRC has investigated this issue and concluded that this does not pose an immediate threat that requires urgent attention due to limited impact. User enumeration does not meet the bar for servicing, as there are multiple ways to check if a user exists or not, with the pre-requisite that the attacker would need to have the specific username. Regarding sign-in not being logged, this is by design for now. We have shared the report with the team responsible for maintaining the product or service. They will review for a potential fix and take appropriate action as needed to help keep customers protected.

We have closed this case. If you have any questions or concerns, please feel free to reach out.

Result

- Lot of publicity
- Logging improvements
- Smart Lockout
- Lessons learned:
  - Enumeration = feature
  - Keep researchers updated
  - Do not lie to researchers
  - It is okay to ask to postpone..



THREAT ANALYSIS

UNDETECTED AZURE ACTIVE DIRECTORY BR

Counter Threat
September 29,

HIT ME BABY ONE MORE TIME —

New Azure Active Directory password brute-forcing flaw has no fix

Micr

AX SHA

TRENDING: Live In-Person Event - Financial Services Cybersecurity Summit Oct. 17th • First Annual Generative

Access Management , Account Takeover Fraud , Fraud Management & Cybercrime

Microsoft Will Mitigate Brute-Force Bug in Azure AD

Microsoft Sparred with SecureWorks Over Impact But Relents

Jeremy Kirk (jeremy_kirk) · September 30, 2021

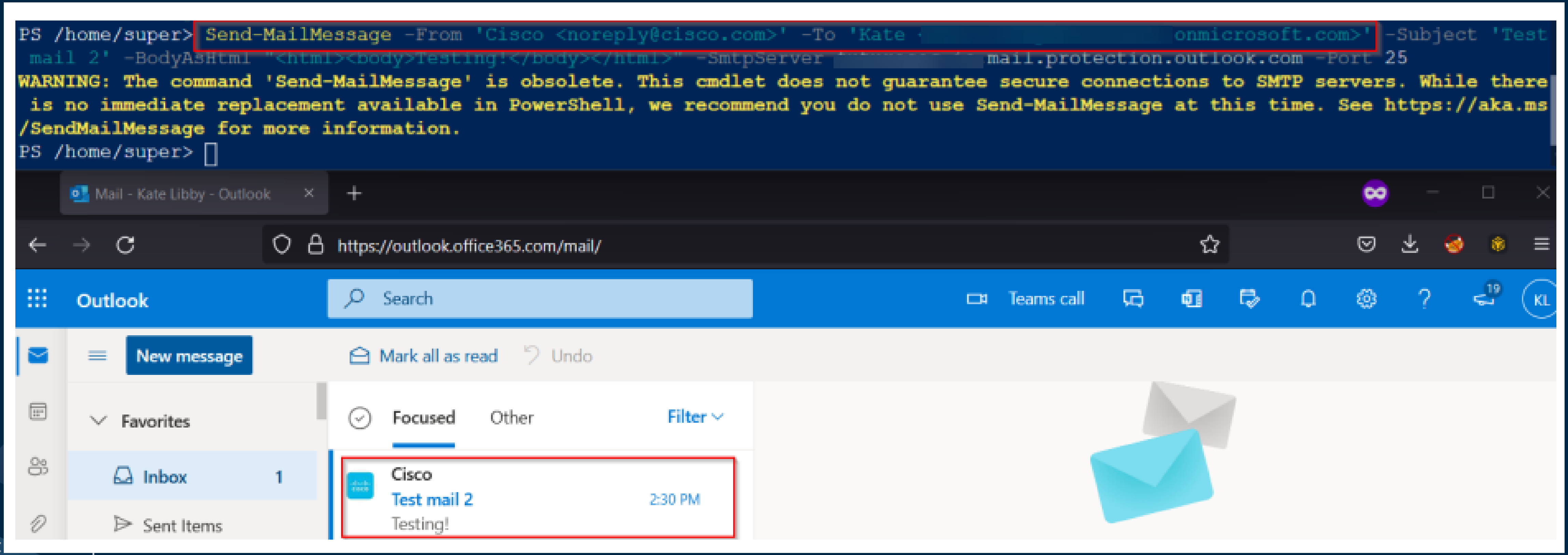
EXO Direct Send

Dec 2021

@424f424f (rvrsh3ll)

Exchange Online Direct Send

- Endpoint allowing multifunction devices to send email via EXO
  - Enabled for all domains: ***company-com*.mail.protection.outlook.com**
  - Allows **anonymously** spoofing emails as any email address target organization trusts



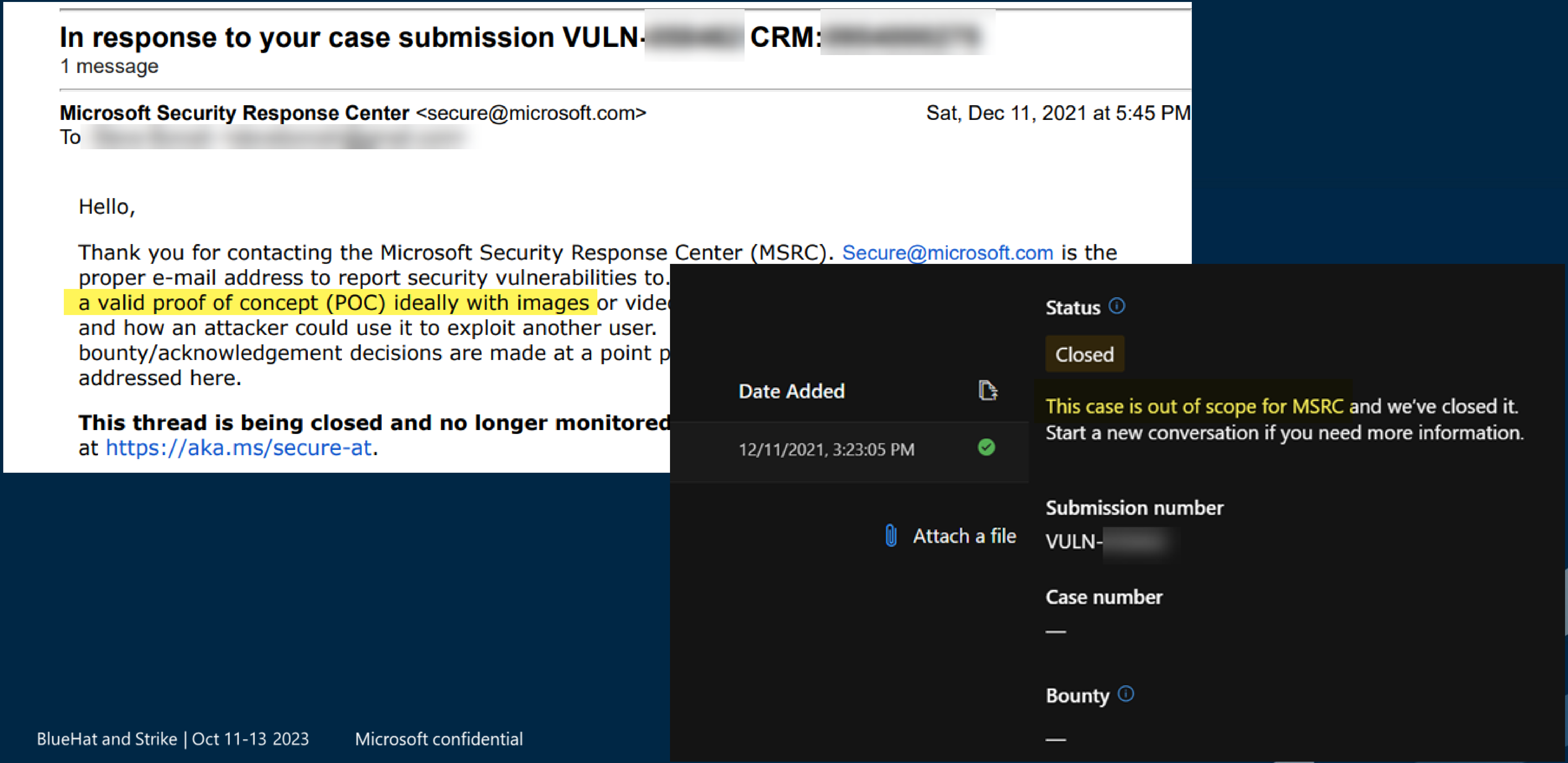
```
PS /home/super> Send-MailMessage -From 'Cisco <noreply@cisco.com>' -To 'Kate [redacted]onmicrosoft.com>' -Subject 'Test
 mail 2' -BodyAsHtml "<html><body>Testing!</body></html>" -SmtpServer [redacted]mail.protection.outlook.com -Port 25
WARNING: The command 'Send-MailMessage' is obsolete. This cmdlet does not guarantee secure connections to SMTP servers. While there
 is no immediate replacement available in PowerShell, we recommend you do not use Send-MailMessage at this time. See https://aka.ms
/SendMailMessage for more information.
PS /home/super> 
```

Cisco
Test mail 2 2:30 PM
Testing!

MITRE ATT&CK

- Initial Access (TA0001)
  - Phishing (T1566)
  - .001 Spearphishing Attachment
  - .003 Spearphishing Link

Response



In response to your case submission VULN-[redacted] CRM:[redacted]
1 message

Microsoft Security Response Center <secure@microsoft.com> Sat, Dec 11, 2021 at 5:45 PM
To [redacted]

Hello,

Thank you for contacting the Microsoft Security Response Center (MSRC). Secure@microsoft.com is the proper e-mail address to report security vulnerabilities to.
a valid proof of concept (POC) ideally with images or vide
and how an attacker could use it to exploit another user.
bounty/acknowledgement decisions are made at a point p
addressed here.

This thread is being closed and no longer monitored
at https://aka.ms/secure-at.

Status ⓘ

Closed

This case is out of scope for MSRC and we've closed it. Start a new conversation if you need more information.

Date Added	
12/11/2021, 3:23:05 PM	✓

Submission number
VULN-[redacted]

Case number
—

Bounty ⓘ
—

Result

- Blog post
- Microsoft contacted employer

- Lessons learned:
  - Don’t close case automatically
  - Don’t contact employers

BHIS
BLOG:
Spoofing Microsoft 365 Like It’s 1995
BLACK HILLS | Information Security
00593

Dumping Global Admins

Feb 2022 – May 2022

Sravan Akkaram @SravanAkkaram · 2h

Finally I got chance to meet the legend @DrAzureAD 🤗

@SravanAkkaram

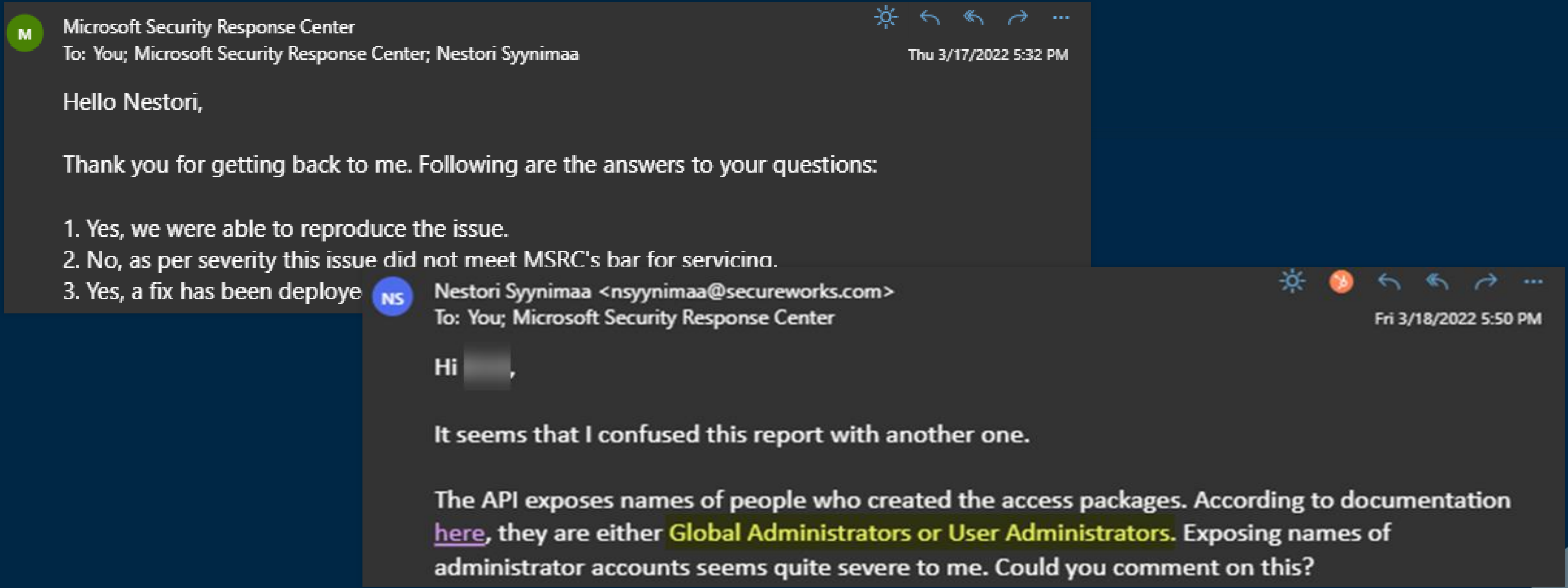
Access Packages

- Allows requesting and approving access to organization’s resources
  - Outsiders, guests, and members
- Back-end API allows:
  - Listing **all** catalogs and access packages as anonymous user
  - CreatedBy and ModifiedBy users were **Global Administrator** or **User Administrators**

MITRE ATT&CK

- Reconnaissance (TA0043)
  - Gather Victim Identity Information (T1589)
  - .002 Email Addresses
  - .003 Employee Names
- Discovery (TA0007)
  - Account Discover (T1087)
  - .004 Cloud Account

Response



Microsoft Security Response Center
To: You; Microsoft Security Response Center; Nestori Syynimaa
Thu 3/17/2022 5:32 PM

Hello Nestori,

Thank you for getting back to me. Following are the answers to your questions:

1. Yes, we were able to reproduce the issue.
2. No, as per severity this issue did not meet MSRC's bar for servicing.
3. Yes, a fix has been deploye

Nestori Syynimaa <nsyynimaa@secureworks.com>
To: You; Microsoft Security Response Center
Fri 3/18/2022 5:50 PM

Hi [redacted],

It seems that I confused this report with another one.

The API exposes names of people who created the access packages. According to documentation here, they are either Global Administrators or User Administrators. Exposing names of administrator accounts seems quite severe to me. Could you comment on this?

Result

- Users can only list packages they are entitled to
  - Package creator (admin) names still available..
- 7k bounty!
- Lessons learned:
  - Argue using documentation
  - Ask for help

Abusing Azure AD Connect

Jun 2020 – Nov 2021

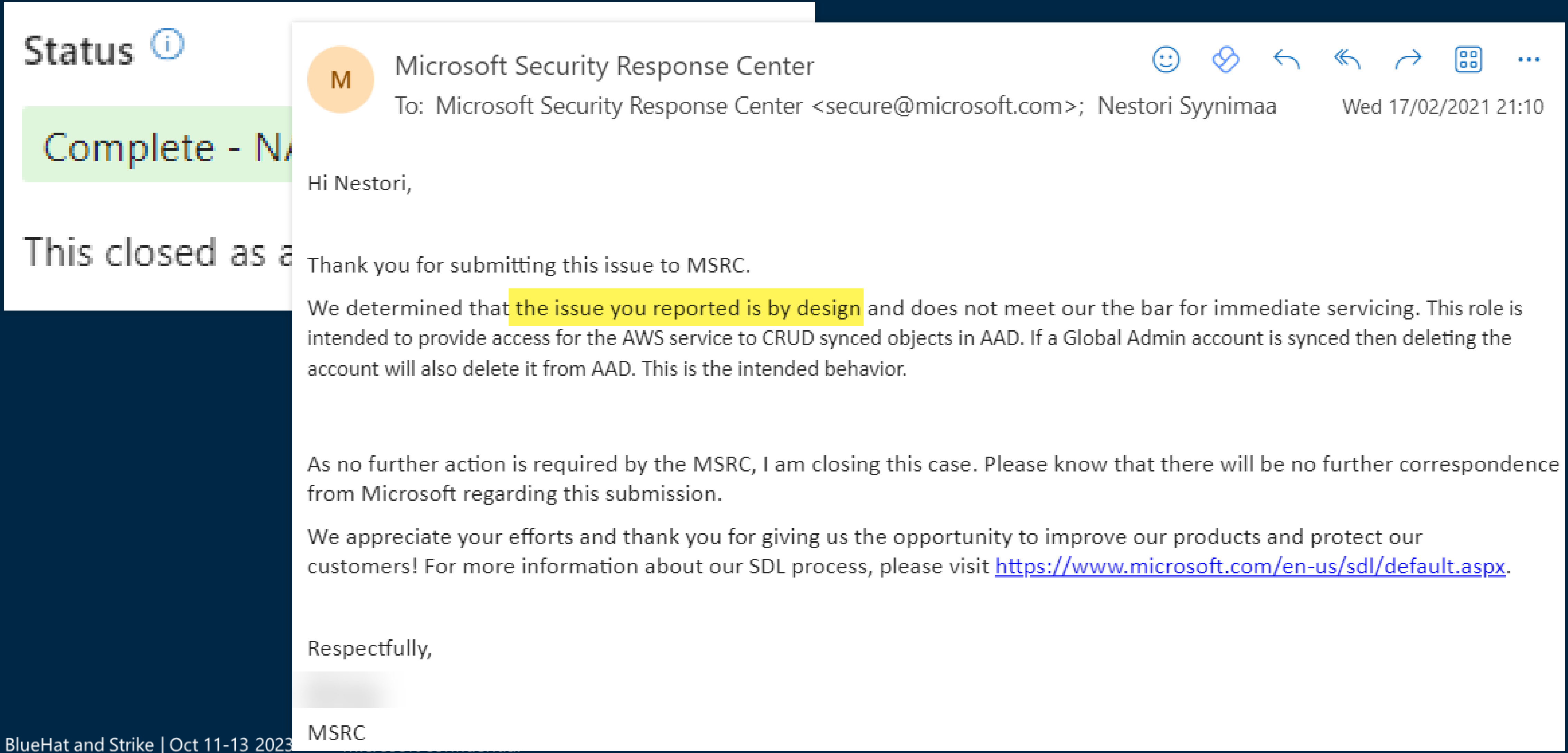
Abusing Azure AD Connect

- Azure AD Connect uses synchronization API to
  - Synchronize users and password hashes from on-prem AD to ~~Azure AD~~ Entra ID
  - Uses **ImmutableID** (aka **SourceAnchor**), B64(GUID)
  - API also supports **CloudAnchor,** “User_ObjectId”
- API allowed
  - CRUDing of cloud-only users
  - Setting passwords of cloud-only users

MITRE ATT&CK

- Privilege Escalation (TA0004)
  - Exploitation for Privilege Escalation (T1068)

Response



Status

Complete - N

This closed as a

Microsoft Security Response Center

To: Microsoft Security Response Center <secure@microsoft.com>; Nestori Syynimaa

Wed 17/02/2021 21:10

Hi Nestori,

Thank you for submitting this issue to MSRC.

We determined that the issue you reported is by design and does not meet our the bar for immediate servicing. This role is intended to provide access for the AWS service to CRUD synced objects in AAD. If a Global Admin account is synced then deleting the account will also delete it from AAD. This is the intended behavior.

As no further action is required by the MSRC, I am closing this case. Please know that there will be no further correspondence from Microsoft regarding this submission.

We appreciate your efforts and thank you for giving us the opportunity to improve our products and protect our customers! For more information about our SDL process, please visit https://www.microsoft.com/en-us/sdl/default.aspx.

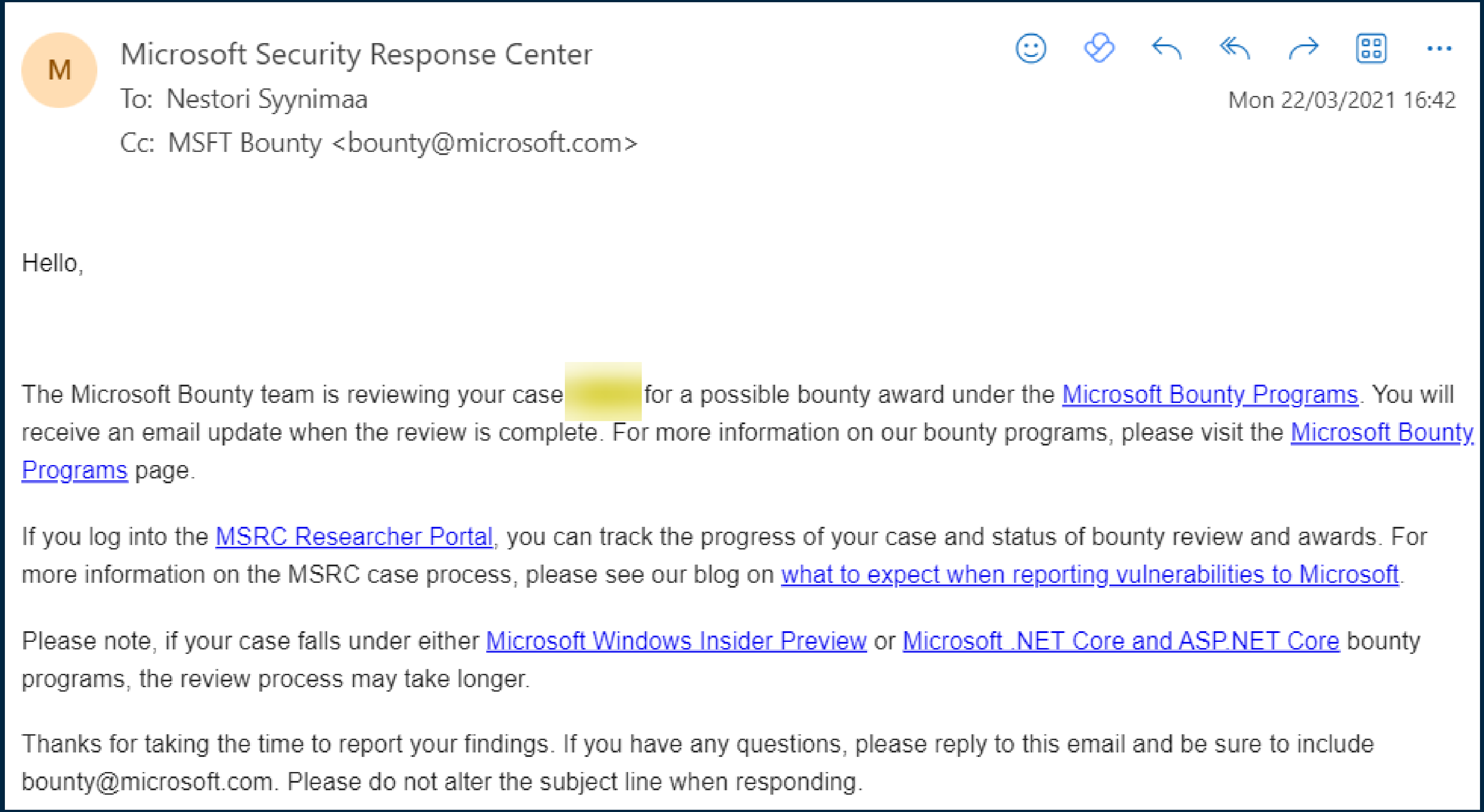
Respectfully,

[redacted]

MSRC

Result 1/2

- Bug fixed
- 20k bounty!
- Lessons learned
  - Read the response
  - Be persistent



M

Microsoft Security Response Center

To: Nestori Syynimaa

Cc: MSFT Bounty <bounty@microsoft.com>

Mon 22/03/2021 16:42

Hello,

The Microsoft Bounty team is reviewing your case [redacted] for a possible bounty award under the Microsoft Bounty Programs. You will receive an email update when the review is complete. For more information on our bounty programs, please visit the Microsoft Bounty Programs page.

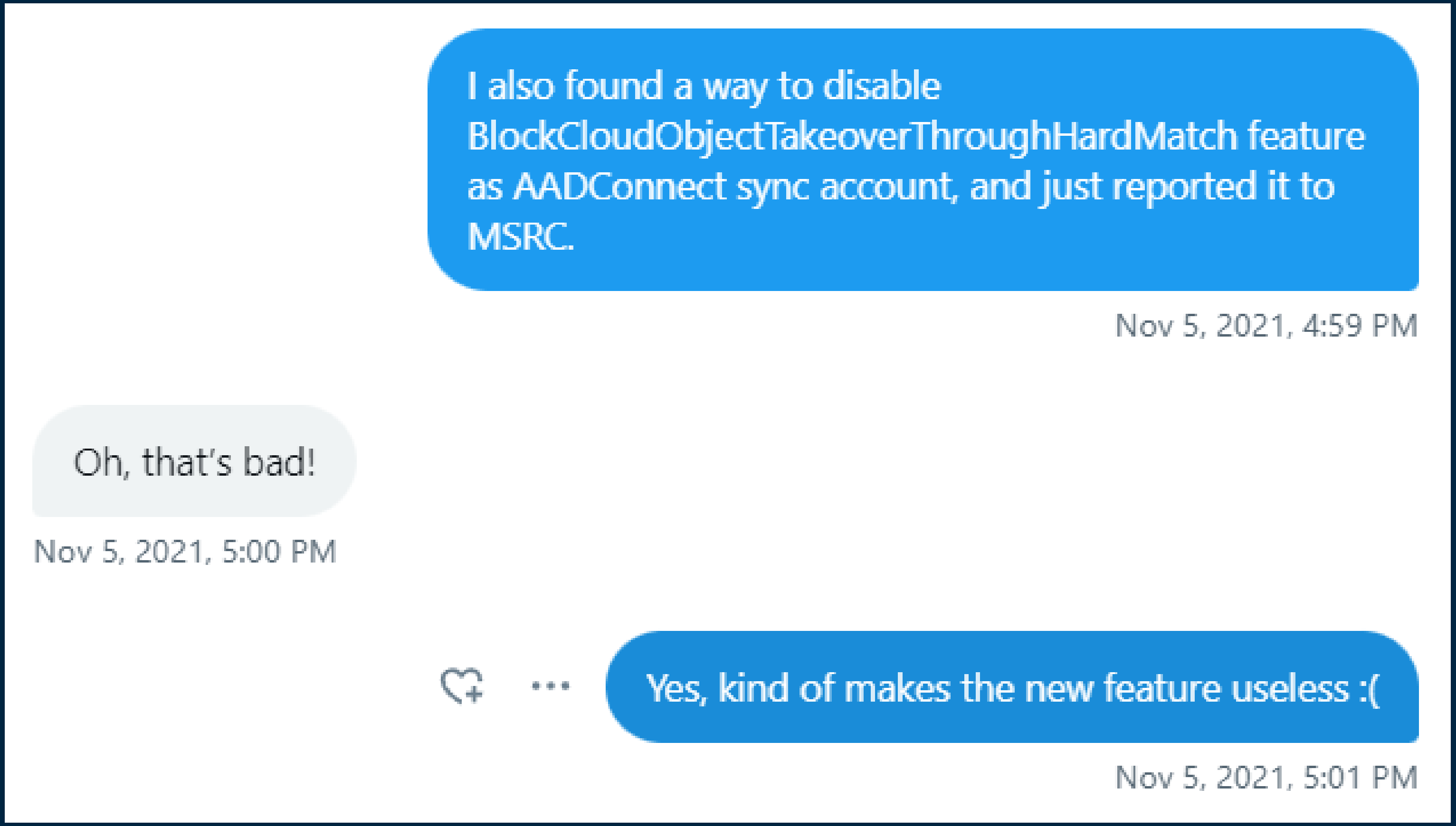
If you log into the MSRC Researcher Portal, you can track the progress of your case and status of bounty review and awards. For more information on the MSRC case process, please see our blog on what to expect when reporting vulnerabilities to Microsoft.

Please note, if your case falls under either Microsoft Windows Insider Preview or Microsoft .NET Core and ASP.NET Core bounty programs, the review process may take longer.

Thanks for taking the time to report your findings. If you have any questions, please reply to this email and be sure to include bounty@microsoft.com. Please do not alter the subject line when responding.

The fix

- A new feature: "BlockCloudObjectTakeoverThroughHardMatch"
  - Prevents manipulating cloud-only users



I also found a way to disable BlockCloudObjectTakeoverThroughHardMatch feature as AADConnect sync account, and just reported it to MSRC.

Nov 5, 2021, 4:59 PM

Oh, that's bad!

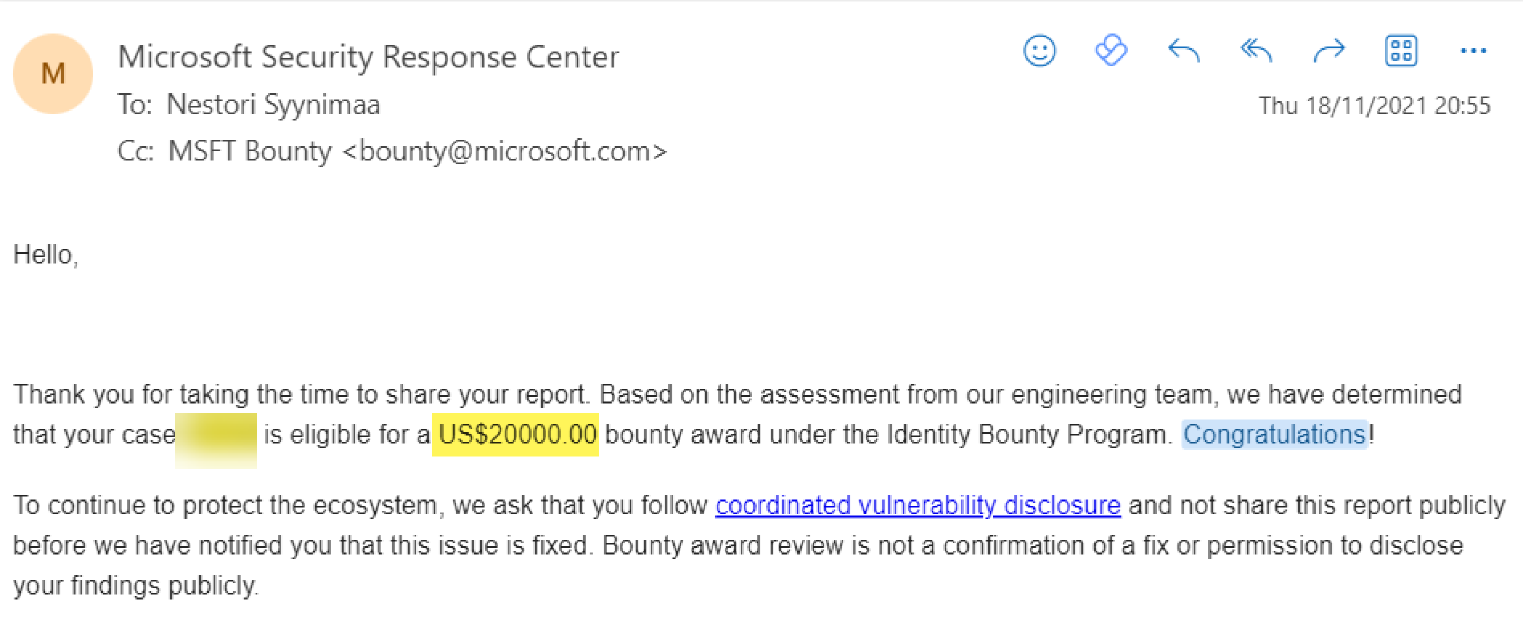
Nov 5, 2021, 5:00 PM

Yes, kind of makes the new feature useless :(

Nov 5, 2021, 5:01 PM

Result 2/2

- Bug fixed
- 20k bounty!
- Lessons learned
  - Check the fix
  - Report in new report
  - Ask researcher to confirm



M

Microsoft Security Response Center

To: Nestori Syynimaa

Cc: MSFT Bounty <bounty@microsoft.com>

Thu 18/11/2021 20:55

Hello,

Thank you for taking the time to share your report. Based on the assessment from our engineering team, we have determined that your case [redacted] is eligible for a US$20000.00 bounty award under the Identity Bounty Program. Congratulations!

To continue to protect the ecosystem, we ask that you follow coordinated vulnerability disclosure and not share this report publicly before we have notified you that this issue is fixed. Bounty award review is not a confirmation of a fix or permission to disclose your findings publicly.

Breaking SPO integrity

Nov 2022 – Aug 2023

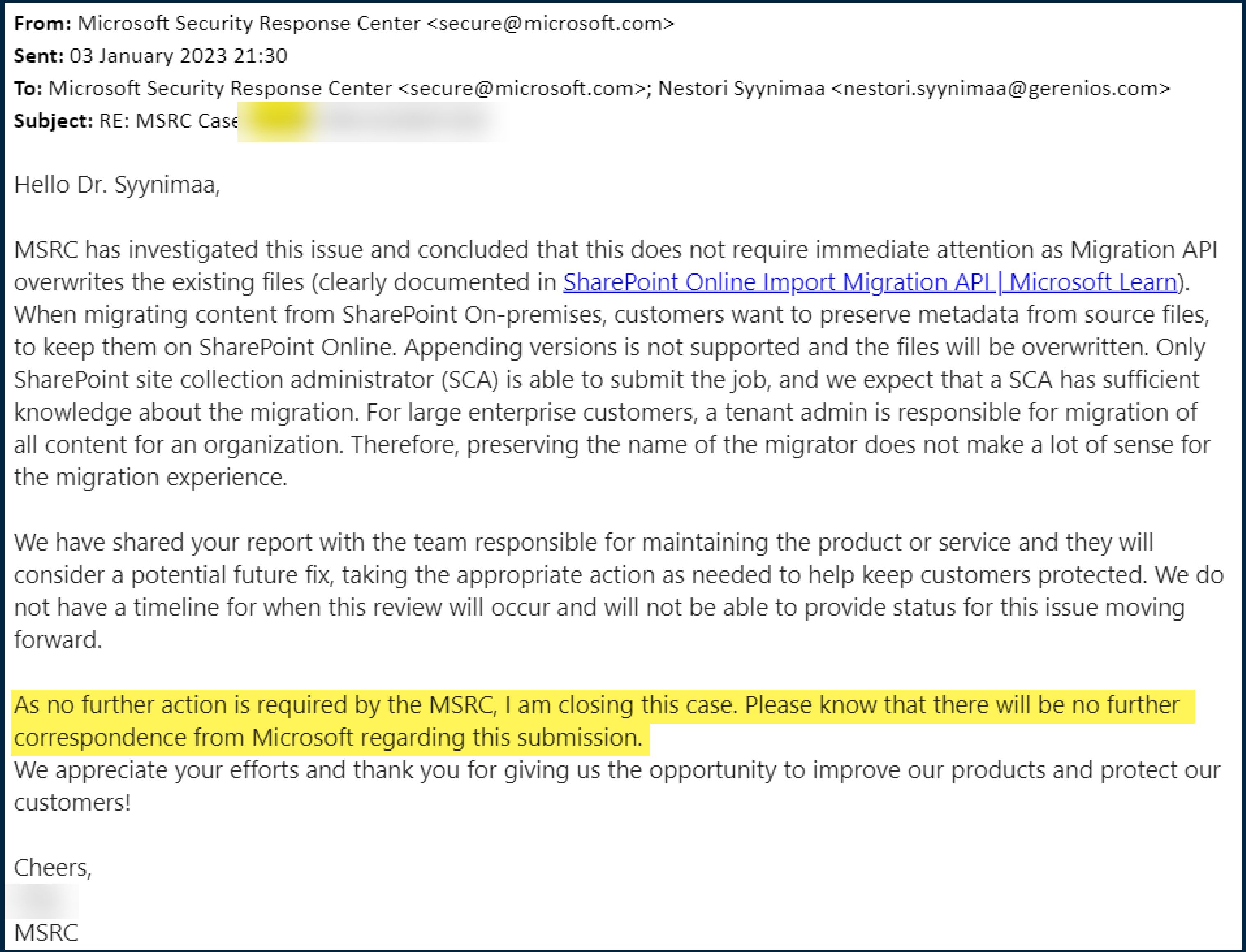
Breaking SPO integrity 1/2

- SharePoint Migration Tool (SPMT) uses “migration API”
  - Full control of metadata (timestamps & created/modified)
  - Creation/modification not logged
  - Requires Site owner permissions (e.g., Team owner)
- API allowed undetected
  - Spoofing of files
  - Tampering with existing files

MITRE ATT&CK

- Impact (TA0040)
  - Data Manipulation (T1565)
  - .001 Stored Data Manipulation
- Privilege Escalation (TA0004)
  - Exploitation for Privilege Escalation (T1068)

Response



From: Microsoft Security Response Center <secure@microsoft.com>
Sent: 03 January 2023 21:30
To: Microsoft Security Response Center <secure@microsoft.com>; Nestori Syynimaa <nestori.syynimaa@gerenios.com>
Subject: RE: MSRC Case [redacted]

Hello Dr. Syynimaa,

MSRC has investigated this issue and concluded that this does not require immediate attention as Migration API overwrites the existing files (clearly documented in [SharePoint Online Import Migration API | Microsoft Learn]). When migrating content from SharePoint On-premises, customers want to preserve metadata from source files, to keep them on SharePoint Online. Appending versions is not supported and the files will be overwritten. Only SharePoint site collection administrator (SCA) is able to submit the job, and we expect that a SCA has sufficient knowledge about the migration. For large enterprise customers, a tenant admin is responsible for migration of all content for an organization. Therefore, preserving the name of the migrator does not make a lot of sense for the migration experience.

We have shared your report with the team responsible for maintaining the product or service and they will consider a potential future fix, taking the appropriate action as needed to help keep customers protected. We do not have a timeline for when this review will occur and will not be able to provide status for this issue moving forward.

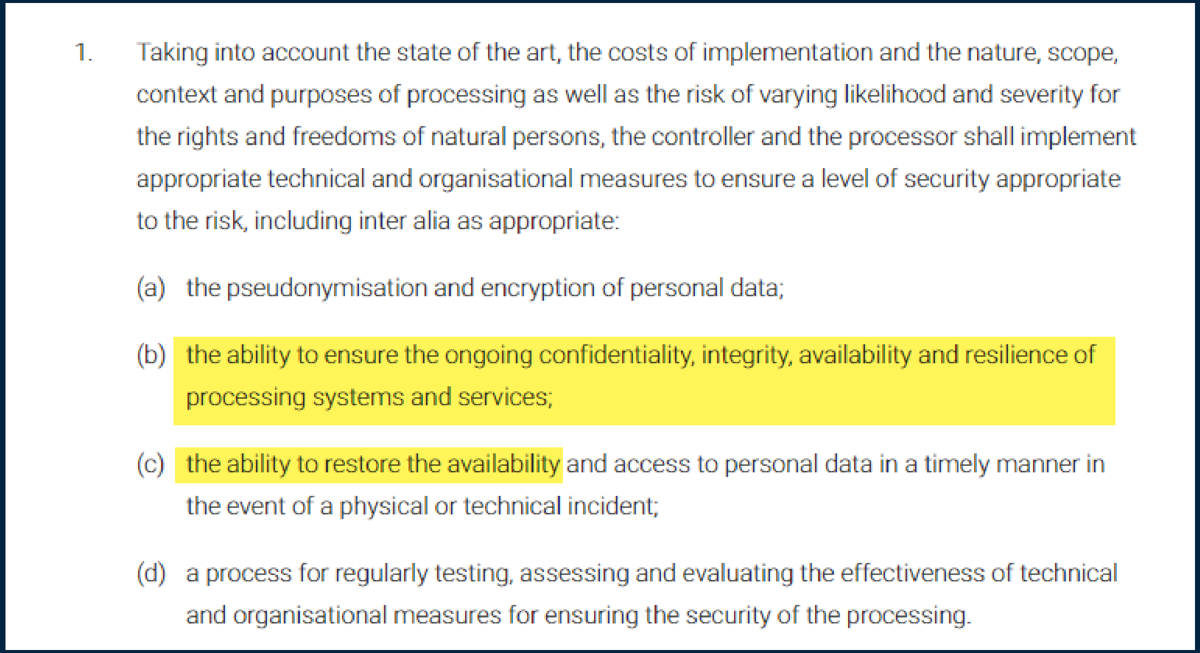
As no further action is required by the MSRC, I am closing this case. Please know that there will be no further correspondence from Microsoft regarding this submission.
We appreciate your efforts and thank you for giving us the opportunity to improve our products and protect our customers!

Cheers,
[redacted]
MSRC

Result 1/2

- Exploitable by regular users who created a Team
  - Cannot be switched off
  - SPO not compliant with several laws / regulations
  - GDPR, HIPAA, ..
- Lessons learned
  - Look outside-the-box

GDPR



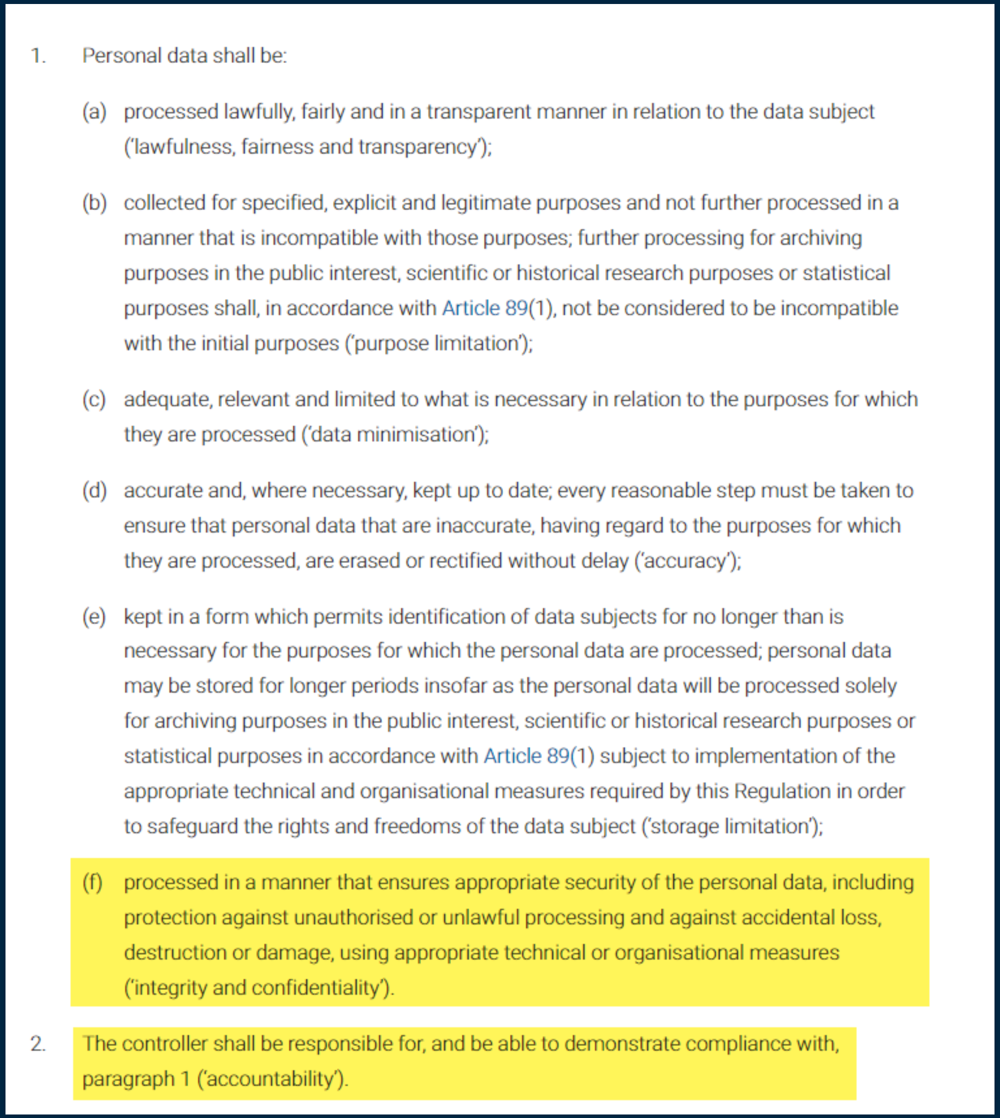
1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

   (a) the pseudonymisation and encryption of personal data;

   (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.



1. Personal data shall be:

   (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

   (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

   (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

   (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

   (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

   (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Breaking SPO integrity 2/2

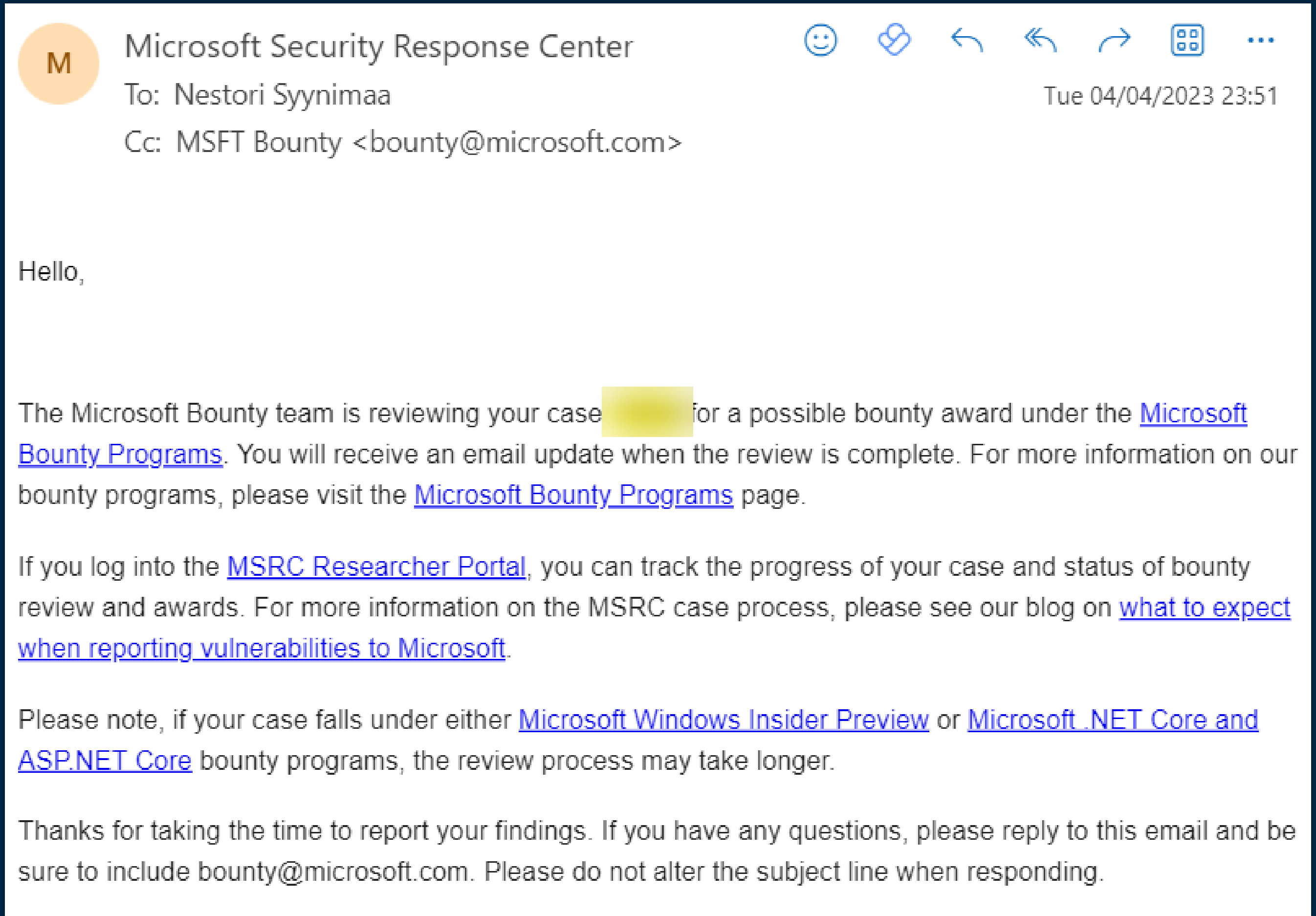
- API allowed undetected
  - Spoofing of files
  - Tampering with existing files, including SPO design files (*.aspx)
- Enabled XSS attacks

MITRE ATT&CK

- Execution (TA0002)
  - Command and Scripting Interpreter (T1059)
  - .007 JavaScript
  - .009 Cloud API
- Initial Access (TA0004)
  - Drive-by Compromise (T1189)
- Defense Evasion (TA0005)
  - Exploitation for Defense Evasion (T1211)

Result 2/2

- Fixed
- 3k bounty!
- Fix didn't work..
  - New fix 2 days before DefCon talk
- Lessons learned
  - Be persistent
  - Remember to submit a new report



M

Microsoft Security Response Center

To: Nestori Syynimaa

Cc: MSFT Bounty <bounty@microsoft.com>

Tue 04/04/2023 23:51

Hello,

The Microsoft Bounty team is reviewing your case [redacted] for a possible bounty award under the Microsoft Bounty Programs. You will receive an email update when the review is complete. For more information on our bounty programs, please visit the Microsoft Bounty Programs page.

If you log into the MSRC Researcher Portal, you can track the progress of your case and status of bounty review and awards. For more information on the MSRC case process, please see our blog on what to expect when reporting vulnerabilities to Microsoft.

Please note, if your case falls under either Microsoft Windows Insider Preview or Microsoft .NET Core and ASP.NET Core bounty programs, the review process may take longer.

Thanks for taking the time to report your findings. If you have any questions, please reply to this email and be sure to include bounty@microsoft.com. Please do not alter the subject line when responding.

Bypassing MFA & CA with EXO API

Oct 2021

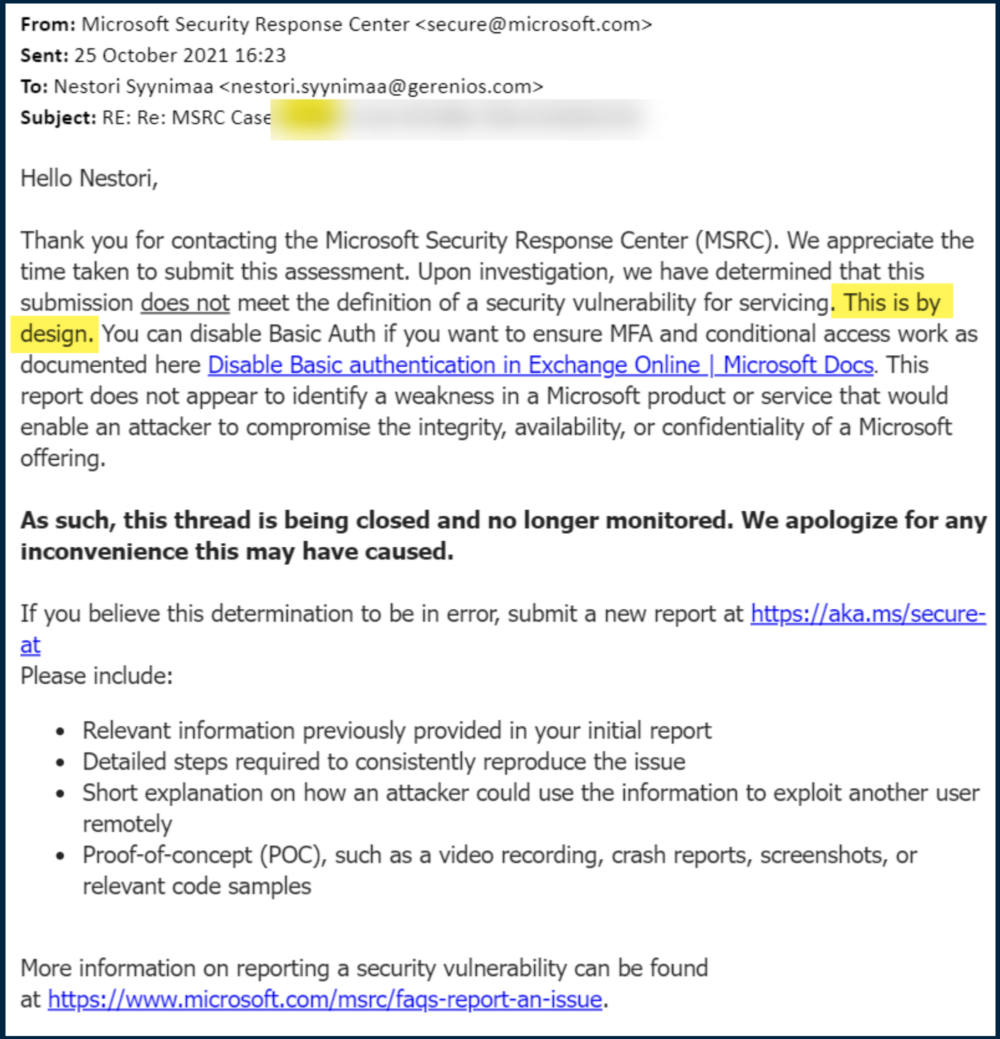
Bypassing MFA & CA with EXO API

- EXO remote PS supports Basic authentication API
  - Allowed bypassing MFA and Conditional Access

MITRE ATT&CK

- Defense Evasion (TA0005)
  - Exploitation for Defense Evasion (T1211)

Response



From: Microsoft Security Response Center <secure@microsoft.com>
Sent: 25 October 2021 16:23
To: Nestori Syynimaa <nestori.syynimaa@gerenios.com>
Subject: RE: Re: MSRC Case [redacted]

Hello Nestori,

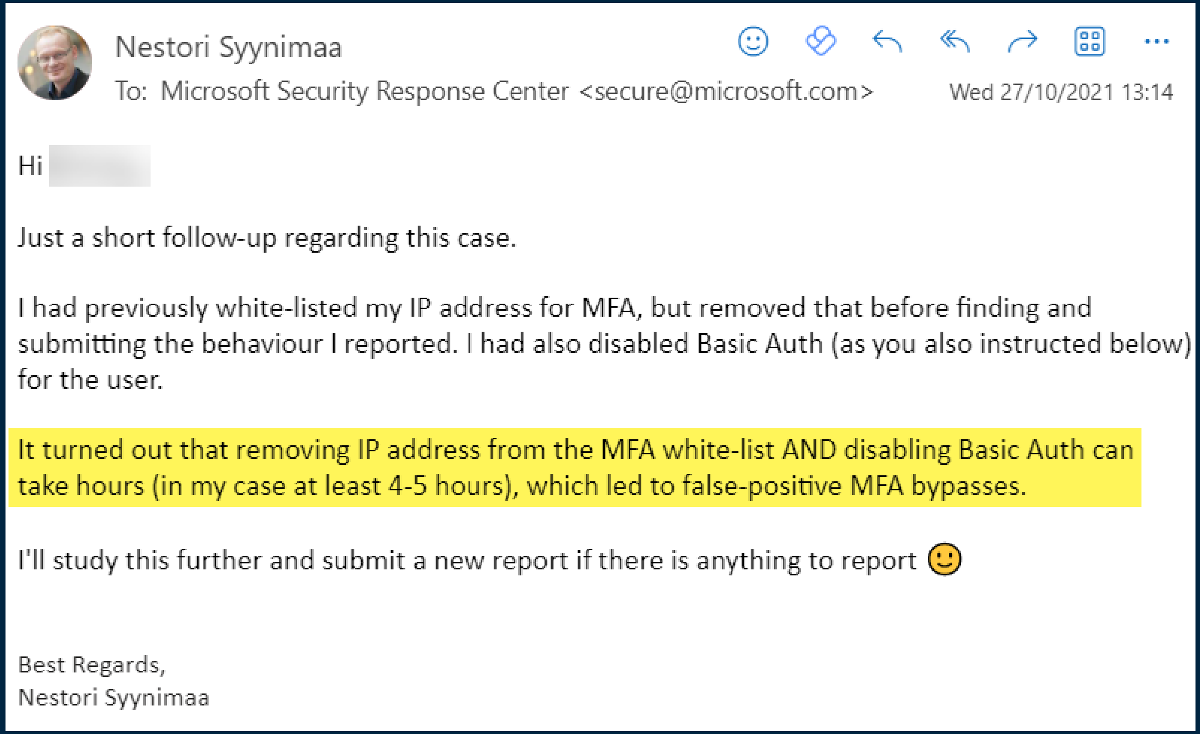
Thank you for contacting the Microsoft Security Response Center (MSRC). We appreciate the time taken to submit this assessment. Upon investigation, we have determined that this submission does not meet the definition of a security vulnerability for servicing. This is by design. You can disable Basic Auth if you want to ensure MFA and conditional access work as documented here [Disable Basic authentication in Exchange Online | Microsoft Docs](). This report does not appear to identify a weakness in a Microsoft product or service that would enable an attacker to compromise the integrity, availability, or confidentiality of a Microsoft offering.

As such, this thread is being closed and no longer monitored. We apologize for any inconvenience this may have caused.

If you believe this determination to be in error, submit a new report at https://aka.ms/secure-at
Please include:

- Relevant information previously provided in your initial report
- Detailed steps required to consistently reproduce the issue
- Short explanation on how an attacker could use the information to exploit another user remotely
- Proof-of-concept (POC), such as a video recording, crash reports, screenshots, or relevant code samples

More information on reporting a security vulnerability can be found at https://www.microsoft.com/msrc/faqs-report-an-issue.



Nestori Syynimaa
To: Microsoft Security Response Center <secure@microsoft.com> Wed 27/10/2021 13:14

Hi [redacted]

Just a short follow-up regarding this case.

I had previously white-listed my IP address for MFA, but removed that before finding and submitting the behaviour I reported. I had also disabled Basic Auth (as you also instructed below) for the user.

It turned out that removing IP address from the MFA white-list AND disabling Basic Auth can take hours (in my case at least 4-5 hours), which led to false-positive MFA bypasses.

I'll study this further and submit a new report if there is anything to report 🙂

Best Regards,
Nestori Syynimaa

Result

- False positive
- Lessons learned:
  - RTFM & double-check

Summary

Microsoft

- Keep researchers updated
- It is okay to ask to postpone
- Do not lie to researchers
- Do not contact employers
- Ask the researcher to validate the fix
- Look outside-the-box

Researcher

- Read the “by-design” response carefully
- Be persistent
- Argue using documentation & previous cases
- Talk to other researchers / ask for help
- Report fix by-pass in a new report
- RTFM & double-check before submitting

Microsoft

MSRC BLUEHAT OCT '23