



Detection and Response for HAFNIUM Activity

 Elastic Security

devonkerr Elastic Team Member

9  Mar 2021



Detection and Response for HAFNIUM Activity

Executive summary

On March 2, 2021, Microsoft released a security update for on-premises Exchange servers to address vulnerabilities being exploited. Security vendors are seeing these vulnerabilities being actively exploited, confirming an imminent threat of leaving systems un-patched. Elastic Security Intelligence & Analytics shares information about detections for this activity, and observations about exploitation in the wild.

Details

On March 2, 2021, Microsoft released a [security update](#) ²³ describing several 0day exploits targeting on-premises Microsoft Exchange servers. Four published vulnerabilities relate to this activity, for which Microsoft released a [patch](#) ¹. The vulnerabilities include [CVE-2021-26855](#) ²⁰, [CVE-2021-26857](#) ⁷, [CVE-2021-26858](#) ¹⁰, and [CVE-2021-27065](#) ⁷.

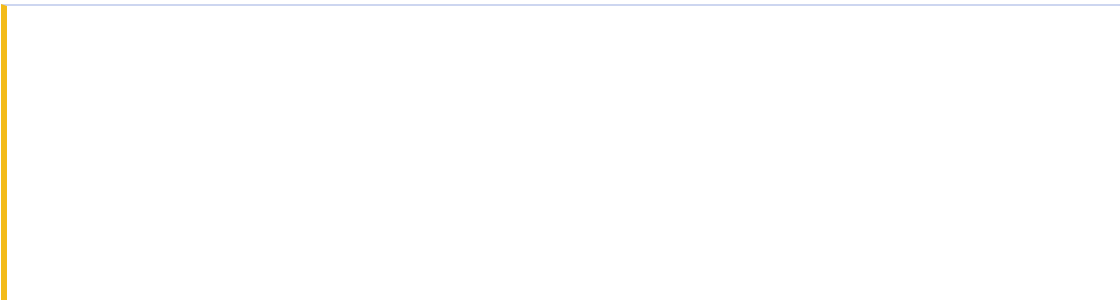
As reported by [Volexity](#) ²⁹ and other security vendors, adversaries exploiting these vulnerabilities may install webshells that function as backdoors. With privileges of the IIS web server, adversaries harvested credentials, conducted reconnaissance, extracted and stole MailBox content and created new users. Elastic Security Intelligence & Analytics has summarized capabilities related to these behaviors to address affected users.

Elastic has also observed evidence of this activity in our telemetry, and we’ve contacted affected customers. One behavior we observed was the deletion of the administrator account from the “Exchange Organization administrators” group (Figure 1) .



Figure 1 - Process ancestry of net group command removing administrator account

Threat researchers observed unusual descendants (“cmd.exe”, “powershell.exe”) of the Exchange IIS webserver (“w3wp.exe”) that involved remote network connections (86.105.18[.]116). Our observations have been independently corroborated by [others](#) ¹⁸ in the community (Figure 2) as malicious. While this activity resembles the HAFNIUM activity group, these observations may represent opportunistic or other threats.



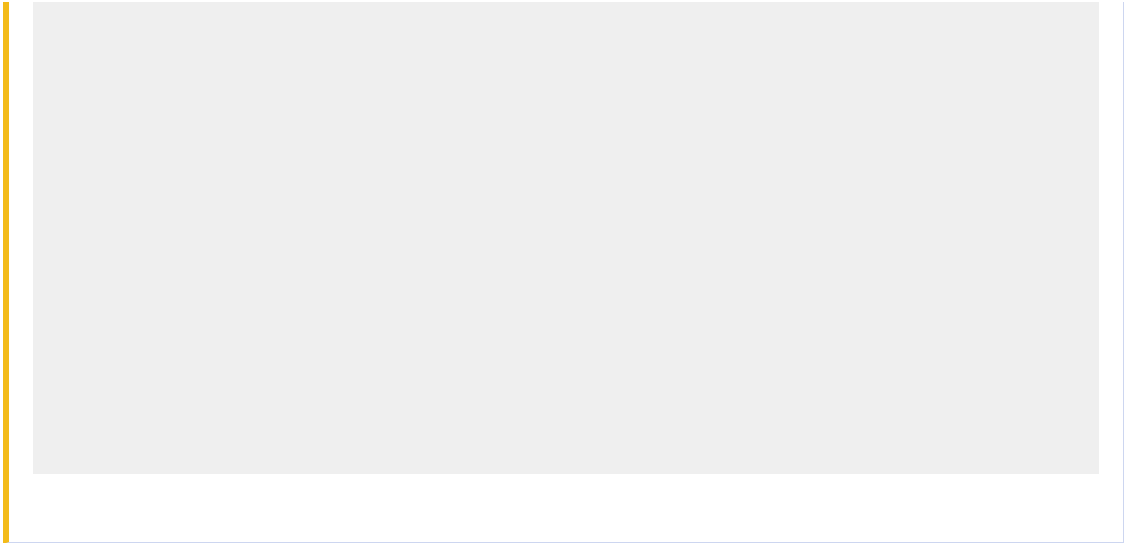


Figure 2 - Adversary download of malicious BATCH script, observed by Elastic

Elastic found that adversaries ran a malicious BATCH script (“1.bat”) which downloaded a legitimate version of the Opera browser (“opera_browser.exe”) and a malicious DLL (“opera_browser.dll”) before launching MSIExec (“msiexec.exe”). On execution, the Opera browser automatically loaded the malicious DLL due to a side-loading vulnerability, then injected shellcode into MSIExec.

Overview

- National Institute of Standards and Technology (NIST) assigned a critical CVSS score of 7.8 - 9.1 out of 10 based on remote code execution without authentication
- The vulnerability affects on-premises Exchange servers which are self-managed
- The initial activity was reported by Microsoft and attributed to “HAFNIUM,” which Microsoft describes as a China-based threat; note general adoption of this methodology by opportunistic threats is likely

Timeline of events

- March 2, 2021 - CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 issued to vulnerability
- March 2, 2021 - Microsoft released patch
- March 3, 2021 - Elastic observes post-exploitation activity via telemetry
- March 4, 2021 - Elastic releases related public detection logic

Impact

Microsoft asserts that these vulnerabilities affect all on-premises Exchange servers (Exchange Server 2013, Exchange Server 2016 and Exchange Server 2019) and issued an update for Microsoft Exchange Server 2010 for completeness. Exchange Online is not affected.

Notably, the initial attack requires on-premises Exchange servers to be accessible to the public Internet via port 443. Attackers with access to enterprises where Exchange servers are internally accessible may be able to exploit unpatched vulnerabilities related to this activity.

The associated HAFNIUM exploit chain leverages multiple tactics and techniques categorized by the MITRE ATT&CK® framework:

- Tactics
 - Credential Access 57
 - Collection 8
 - Command and Control 14
 - Execution 3

- [Lateral Movement](#) 26
 - [Persistence](#) 14
- Techniques/Subtechniques
 - [OS Credential Dumping](#) 12
 - [Email Collection](#) 5
 - [Archive Collected Data](#) 5
 - [Web Service](#) 5
 - [System Services](#) 2 /[Service Execution](#) 1
 - [Remote Services](#) 2
 - [Create Account](#) 7

Detection

Detection logic

On March 4, 2021, Elastic released guidance describing Elastic Endpoint rules that target this cluster of activity (HAFNIUM) in the public repository:

- [Potential Credential Access via Windows Utilities](#) 137
- [Exporting Exchange Mailbox via PowerShell](#) 53
- [Encrypting Files with WinRar or 7z](#) 36
- [Connection to Commonly Abused Web Services](#) 29
- [PsExec Network Connection](#) 33
- [Suspicious Process Execution via Renamed PsExec Executable](#) 29
- [Remotely Started Services via RPC](#) 23
- [User Account Creation](#) 42

Additionally, two new behavioral rules for Elastic Endpoint have been created in light of this newly reported activity:

- [Microsoft Exchange Server UM Spawning Suspicious Processes](#) 68
- [Microsoft Exchange Server UM Writing Suspicious Files](#) 34

On March 4, 2021, Elastic also released guidance describing Elastic Endgame rules that target this cluster of activity. The following rules can be enabled:

- Creation of an Archive File
- Encrypting Files with 7Zip
- Webshell Detection
- PsExec Lateral Movement Command
- Suspicious PowerShell Downloads
- Enumeration of Administrator Accounts

The following supplemental queries for Elastic Endgame may also be recommended:

Memory Dump via Comsvcs (Endgame EQL):

The detection logic in Figure 1 (below) identifies suspicious or unexpected use of a native application (“rundll32.exe”) to perform a process memory dump. This activity may indicate an attempt to obtain process memory from LSASS, which may contain credentials.

```
process where subtype.create and process_name = "rundll32.exe" and command_line == "MiniDump full"
```

Figure 3 - Memory Dump via Comsvcs

Descendants of IIS (Endgame EQL):

The detection logic in Figure 2 (below) identifies unusual descendants of the IIS webserver process (“w3wp.exe”). This activity may indicate

commands or other observable behaviors related to the use of a persistent webshell.

```
process where subtype.create and parent_process_name = "w3wp.exe"
```

Figure 4 - Descendants of IIS

Creation of an Archive File (Endgame EQL):

The detection logic in Figure 3 (below) identifies file operations related to common archiving utilities. This activity may indicate an attempt to obtain process memory from LSASS, which may contain credentials.

```
file where not subtype.delete and wildcard(file_name, ".7z", ".rar")
```


Figure 5 - Creation of an Archive File


Defensive recommendations

- 1. Review and [implement](#) ³³ the above detection logic within your environment using technology such as Elastic Endpoint, Winlogbeat, Filebeat, Packetbeat, or Network Security Monitoring (NSM) platforms such as Zeek or Suricata.
- 2. Review and ensure that you have deployed the latest Microsoft [Security Updates](#) ¹ for Exchange Server, consider other [recommendations](#) ⁸ from Microsoft for Exchange hardening.
- 3. Maintain backups of your critical systems to aid in quick recovery.
- 4. Perform routine vulnerability scans of your systems and patch identified vulnerabilities.

References

- 1. CVE-2021-26855 | Microsoft Server Remote Code Execution Vulnerability
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855> ²⁰
- 2. CVE-2021-26857 | Microsoft Server Remote Code Execution Vulnerability
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857> ⁷
- 3. CVE-2021-26858 | Microsoft Server Remote Code Execution Vulnerability
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858> ¹⁰
- 4. CVE-2021-27065 | Microsoft Server Remote Code Execution Vulnerability
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065> ⁷
- 5. HAFNIUM targeting Exchange Servers with 0-day exploits
<https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/> ²³
- 6. Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities

 Volexity – 2 Mar 21



Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day... 29

[UPDATE] March 8, 2021 – Since original publication of this blog, Volexity has now observed that cyber espionage operations using the SSRF vulnerability CVE-2021-26855 started occurring on January 3, 2021, three days earlier than initially...

Indicators of Compromise

Table 1 describes atomic indicators of compromise (IOCs) observed in this intrusion-set. IOCs observed by Elastic have been included for the community, and don't represent all IOCs associated with HAFNIUM or HAFNIUM-inspired intrusions.

Artifact	Note	SHA256
Batch Script,		
[shellcode]	Encrypted object	4e3b7cb4cebe2b00645dda08a2:
opera_browser.exe	Legitimate Opera browser application	5aa7c379eb054a745d3c187f8771
opera_browser.dll	Malicious DLL, side-loaded by opera_browser.exe	b212655aeb4700f247070ba5ca6
86.105.18[.]116	Staging site, hosts files used in this activity cluster	N/A

Table 1 - Indicators of Compromise

🔗 2021: The Year in Review

18.9k views

46 links

7 min read

COFFEECOFFEE Michael Koch

Mar 2021

I backported the SIEM rules to 7.10 syntax:
[rules_export_hafnium_7.10_backport.ndjson](#) (github.com) 25



1

👍

🔗



dstepanic Daniel Stepanic Elastic Team Member

1 ✎ Mar 2021

Update - Detection and Response for HAFNIUM Activity

Executive summary



📖 Topics

✎ Drafts

⋮ More

▼ CATEGORIES

📅 Announcements

📘 Elastic Stack

📘 Elastic Search

📘 Elastic Observability

📘 Elastic Security

☰ All categories

▼ TAGS

💎 filebeat

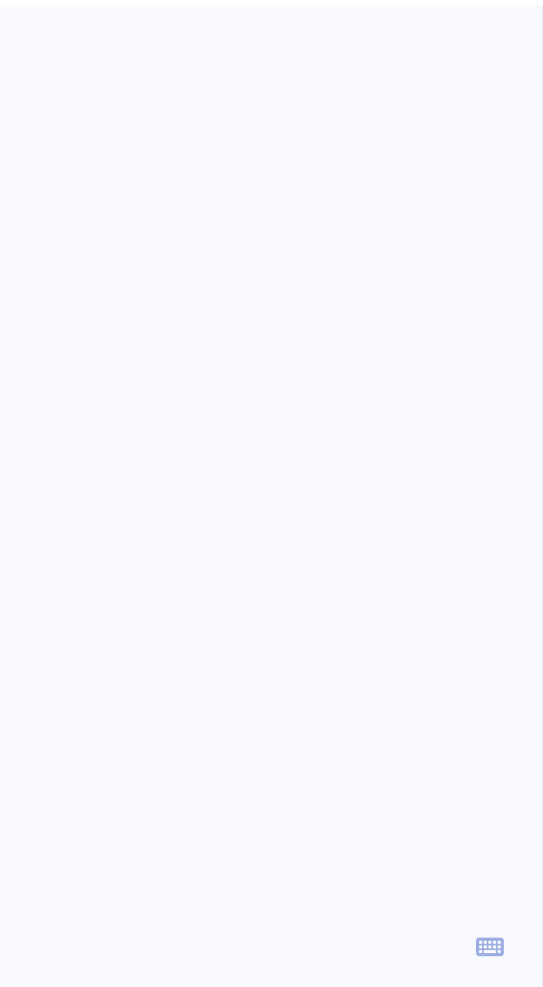
💎 docker

💎 elastic-stack-security

💎 metricbeat

💎 elastic-stack-alerting

☰ All tags



Elastic Security Intelligence & Analytics has identified additional behaviors related to or inspired by HAFNIUM activity, as outlined in the prior [post](#). This update contains additional post-exploitation details observed in Elastic telemetry indicating successful exploitation of recently-disclosed Microsoft Exchange vulnerabilities. While the details of this activity may resemble that attributed to the HAFNIUM threat group, we assess with moderate confidence that opportunistic or other threats are responsible.

Details

On March 4, 2021, Elastic Security identified evidence that Microsoft Exchange vulnerabilities ([CVE-2021-26855](#) ¹, [CVE-2021-26857](#) ¹, [CVE-2021-26858](#) ¹, and [CVE-2021-27065](#) ¹) were being exploited via telemetry; with evidence of compromise as early as February 28, 2021. As we have continued to monitor telemetry for evidence these vulnerabilities were being exploited, we wanted to provide the community with additional information around this cluster of emerging threat activity.

The earliest evidence of observed post-exploitation for this cluster of activity occurred on February 28, 2021. Elastic observed a significant increase in post-exploitation activity related to compromised environments from last week’s published Microsoft Exchange Server vulnerabilities. Threat researchers found inconsistent methodologies present in this activity, which may indicate more than one group pursuing reconnaissance and credential-harvesting objectives.

In several customer environments, adversaries deployed [batch scripts](#) ¹⁹ that automated several functions including account enumeration, credential-harvesting and network discovery. The Security Account Manager (SAM), System and Security hives can be used to obtain plaintext or other credentials. Data staged and stolen from enterprises included similar materials, example commands are depicted in Figure 1:

```
cmd /c reg save hklm\sam C:\windows\temp\debugsms\sam
cmd /c reg save hklm\system C:\windows\temp\debugsms\system
cmd /c reg save hklm\security C:\windows\temp\debugsms\security
```

Figure 1 - Commands used to dump sensitive data from Windows Registry

By collecting this data, the adversary obtains Windows account password hashes and sensitive data that may provide insights into the environment and opportunities for additional lateral movement pivots within the network. Figure 2 depicts a process tree of this activity

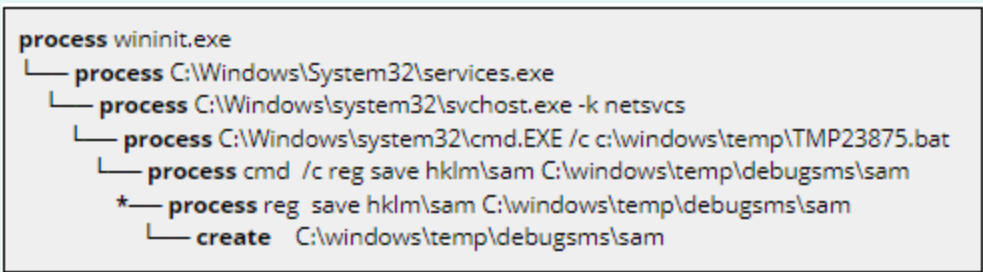


Figure 2 - Process tree of SAM registry hive being dumped

Along with the captured registry hives, network enumeration and discovery data was collected using the following commands in Figure 3.

```
cmd /c ipconfig /all
cmd /c arp -a
```

Figure 3 - Network discovery commands

Reconnaissance output was being staged and compressed on March 8 and March 9 using the Windows [makecab](#) ⁶ utility. Using this tool, adversaries compressed reconnaissance output and hive data together

then altered output files to masquerade as GIF or PNG image files. An example of this command appears in Figure 4.

```
cmd /c makecab /f c:\windows\temp\REDACTED.log /d
compressiontype=lzx /d compressionmemory=21 /d
maxdisksize=1024000000 /d diskdirectorytemplate="C:\Program
Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth"
/d cabinetnametemplate=REDACTED.gif
```

Figure 4 - makecab command used to compress collected data

Below is an image showing the typical contents of these cabinet files in Figure 5.

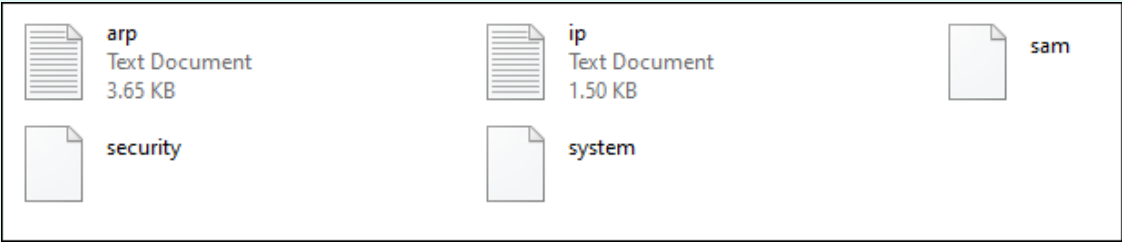


Figure 5 - CAB contents including registry hives and network information

During these periods of activity, adversaries also removed malicious and staged files to prevent their discovery. This behavior was executed through the Exchange IIS webserver process (“w3wp.exe”) and executed almost 24 hours after the registry hives were stolen in some cases. Figure 6 depicts a process lineage in which the adversary uses scripts to clean up after themselves.



Figure 6 - Process tree of cleanup command

Threat researchers identified evidence of adversaries modifying the configuration of Windows Remote Management to enable compatibility listeners, a setting which allows traffic on port 443 as well as starting the WinRM service using the quickconfig command as seen in Figure 7.

```
cmd /c winrm set winrm/config/service
@{EnableCompatibilityHttpsListener="true"}
cmd /c winrm quickconfig -q
```

Figure 7 - WinRM configuration commands

Each of the previously discussed commands were executed in succession triggered through a scheduled task named “WwanSvcdcscs” created from the batch file as depicted in Figure 8.

```
schtasks /create /ru system /tn "\"Microsoft\Windows\WwanSvcdcscs" /tr
"cmd /c c:\windows\temp\TMP23875.bat" /sc once /st 23:59
```

Figure 8 - Scheduled task set-up and execution

Overview

- Elastic Security confirmed that recently disclosed Microsoft Exchange vulnerabilities were being exploited by at least one and

- possibly several threat groups
- Analysis suggests that batch scripts used in more than one instance performed automation of host/network discovery, account enumeration, credential-harvesting, data staging, data theft and tidying functions
- Organizations were targeted in several industries including technical consulting, financial services and entertainment

Timeline of events

- February 28, 2021 - Earliest evidence of Exchange Organization administrator enumeration
- March 2, 2021 - CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065 issued to vulnerability
- March 2, 2021 - Microsoft releases patch
- March 3, 2021 - Earliest attempted post-exploitation activity in several customer environments
- March 4, 2021 - Elastic releases initial Discuss post and public detection logic
- March 5-9, 2021 - Additional post-exploitation activity in customer environments
- March 10, 2021 - Elastic releases follow-up describing newly-observed activity with detection logic

Impact

The post-exploitation behaviors observed leverage multiple tactics and techniques categorized by the MITRE ATT&CK® framework:

- Tactics
 - Credential Access 8
 - Collection
 - Discover 5
 - Execution
 - Persistence 1
 - Defense Evasion 1
- Techniques
 - Automated Collection 3
 - System Network Configuration Discovery
 - OS Credential Dumping 1
 - Scheduled Task/Job 2
 - Indicator Removal on Host 2
 - Archive Collected Data 1

Detection

Detection logic

On March 10, 2021, Elastic released guidance describing Elastic Endpoint rules that target this post-exploitation activity described in the public repository:

- Credential Acquisition via Registry Hive Dumping 19
- Local Scheduled Task Commands 12
- Microsoft Exchange Worker Spawning Suspicious Processes 12

The following supplemental queries for Elastic Endgame may also be recommended:

Suspicious Microsoft Cabinet Maker execution (Endgame EQL)

Identifies the execution of Microsoft Cabinet Maker from suspicious directories or with suspicious process argument, this may indicate data staging activity as a preparation step for exfiltration:

```
process where subtype.create and original_file_name = "makecab.exe"
and wildcard(command_line, "*Microsoft\\Exchange Server\\*",
"*inetpub\\wwwroot*")
```

Figure 9-1 - Suspicious Microsoft Cabinet Maker execution directory

```
process where subtype.create and original_file_name = "makecab.exe"
and wildcard(command_line, "*cabinetnametemplate=*.png",
"*cabinetnametemplate=*.jpg", "*cabinetnametemplate=*.gif",
"*cabinetnametemplate=*.jpeg", "*cabinetnametemplate=*.jpe",
"*cabinetnametemplate=*.bmp")
```

Figure 9-2 - Suspicious Microsoft Cabinet Template Extensions

Suspicious Scheduled Task Creation (Endgame EQL)

Identifies the creation of a scheduled task with suspicious path (tasks within \Microsoft\Windows path are rarely created using schtasks.exe utility):

```
process where subtype.create and original_file_name = "schtasks.exe"
and command_line == "*create* \\Microsoft\\Windows\\"
```

Figure 10 - Suspicious Scheduled Task Creation

For additional detection logic, our first [post](#) related to the HAFNIUM activity is strongly recommended for review.

References

- 1. Detection and Response for HAFNIUM Activity

Detection and Response for HAFNIUM Activity

■ Elastic Security

Detection and Response for HAFNIUM Activity Executive summary On March 2, 2021, Microsoft released a security update for on-premises Exchange servers to address vulnerabilities being exploited. Security vendors are seeing these vulnerabilities being actively exploited, confirming an imminent threat of leaving systems un-patched. Elastic Security Intelligence & Analytics shares information about detections for this activity, and observations about exploitation in the wild. Details On March 2, 20...

- 2. HAFNIUM targeting Exchange Servers with 0-day exploits

<https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/> 5

Indicators of Compromise

Table 1 describes atomic indicators of compromise (IOCs) observed in this intrusion-set. IOCs observed by Elastic have been included for the community, and don't represent all IOCs associated with HAFNIUM or HAFNIUM-inspired intrusions.

Artifact	Note	SHA256
----------	------	--------

xx.bat

Batch Script

2f907f2da760bbadc713d710166a68e73895a75cb695b48

5

6 months later



Closed on Sep 21, 2021

This topic was automatically closed 100 days after the last reply. New replies are no longer allowed.

Reply

New & Unread Topics

Topic	Replies	Activity
How to reopen an accidental closing of all alerts ■ Elastic Security	3	12d
☑ Missing “Custom Fields” in alerts generated from “endpoint” indexes ■ Elastic Security	4	5d
Distinguish between actions in container from action on hosts ■ Elastic Security docker	0	19d
Integration Elasic stack with thehive ■ Elastic Security	2	17d
[ERROR] Winlogbeat cannot connect to Elastic ■ Elastic Security	1	4d

Want to read more? Browse other topics in ■ Elastic Security or view latest topics.