



Elastic Security:

8.15 (current)

Elastic Security overview

What's new in 8.15

Upgrade Elastic Security to 8.15.3

Post-upgrade steps (optional)

Get started with Elastic Security

AI for security

Detections and alerts

Detections prerequisites and requirements

About detection rules

Create a detection rule

Install and manage Elastic prebuilt rules

Manage detection rules

Monitor and troubleshoot rule executions

Rule exceptions

About building block rules

MITRE ATT&CK® coverage

Manage detection alerts

Reduce notifications and alerts

Query alert indices

Tune detection rules

Prebuilt rule reference

A scheduled task was created

A scheduled task was updated

APT Package Manager Configuration File Creation

AWS Bedrock Detected Multiple Attempts to use Denied Models by a Single User

AWS Bedrock Detected Multiple Validation Exception Errors by a Single User

AWS Bedrock Guardrails Detected Multiple Policy Violations Within a Single Blocked Request

AWS Bedrock Guardrails Detected Multiple Violations by a Single User Over a Session

# Windows Service Installed via an Unusual Client



Identifies the creation of a Windows service by an unusual client process. Services may be created with administrator privileges but are executed under SYSTEM privileges, so an adversary may also use a service to escalate privileges from administrator to SYSTEM.

Rule type: eql

Rule indices:

- winlogbeat-\*
- logs-system.\*
- logs-windows.\*

Severity: high

Risk score: 73

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also Additional look-back time)

Maximum alerts per execution: 100

References:

- https://www.x86matthew.com/view\_post?id=create\_svc\_rpc
- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4697
- https://github.com/atc-project/atomic-threat-coverage/blob/master/Atomic\_Threat\_Coverage/Logging\_Policies/LP\_0100\_windows\_audit\_security\_sys
- https://www.elastic.co/security-labs/siestagraph-new-implant-uncovered-in-asean-member-foreign-ministry

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Privilege Escalation
- Data Source: System

Version: 211

Rule authors:

- Elastic

AWS CLI Command with Custom Endpoint URL

AWS CloudTrail Log Created

**Rule license:** Elastic License v2

## Setup



### Setup

The *Audit Security System Extension* logging policy must be configured for (Success) Steps to implement the logging policy with Advanced Audit Configuration:

```
Computer Configuration >
Policies >
Windows Settings >
Security Settings >
Advanced Audit Policies Configuration >
Audit Policies >
System >
Audit Security System Extension (Success)
```

## Rule query



```
configuration where host.os.type == "windows" and
event.action == "service-installed" and
(winlog.event_data.ClientProcessId == "0" or winlog.event_data.ParentProcessId == "0")
not winlog.event_data.ServiceFileName : (
  "?:\Windows\VeeamVssSupport\VeeamGuestHelper.exe",
  "?:\Windows\VeeamLogShipper\VeeamLogShipper.exe",
  "%SystemRoot%\system32\Drivers\CrowdStrike\*-CsInstallerService.exe",
  "\"%windir%\AdminArsenal\PDQInventory-Scanner\service-1\PDQInventory-Scanner.exe"
)
```

**Framework:** MITRE ATT&CK™

- Tactic:
  - Name: Privilege Escalation
  - ID: TA0004
  - Reference URL: <https://attack.mitre.org/tactics/TA0004/>
- Technique:
  - Name: Create or Modify System Process
  - ID: T1543
  - Reference URL: <https://attack.mitre.org/techniques/T1543/>
- Sub-technique:
  - Name: Windows Service
  - ID: T1543.003
  - Reference URL: <https://attack.mitre.org/techniques/T1543/003/>

**ElasticON events are back!**

Learn about the Elastic Search AI Platform from the experts at our live events.

[Learn more](#)

Was this helpful?



The Search AI Company

## Follow us



## About us

[About Elastic](#)  
[Leadership](#)  
[DE&I](#)  
[Blog](#)  
[Newsroom](#)

## Join us

[Careers](#)  
[Career portal](#)

## Partners

[Find a partner](#)  
[Partner login](#)  
[Request access](#)  
[Become a partner](#)

## Trust & Security

[Trust center](#)  
[EthicsPoint portal](#)  
[ECCN report](#)  
[Ethics email](#)

## Investor relations

[Investor resources](#)  
[Governance](#)  
[Financials](#)  
[Stock](#)

## EXCELLENCE AWARDS

[Previous winners](#)  
[ElasticON Tour](#)  
[Become a sponsor](#)  
[All events](#)

[Trademarks](#) [Terms of Use](#) [Privacy](#) [Sitemap](#)

© 2024. Elasticsearch B.V. All Rights Reserved

Elastic, Elasticsearch and other related marks are trademarks, logos or registered trademarks of Elasticsearch B.V. in the United States and other countries.

Apache, Apache Lucene, Apache Hadoop, Hadoop, HDFS and the yellow elephant logo are trademarks of the Apache Software Foundation in the United States and/or other countries. All other brand names, product names, or trademarks belong to their respective owners.