



Start free trial

Contact Sales

[Platform](#) [Solutions](#) [Customers](#) [Resources](#) [Pricing](#) [Docs](#)

[Elastic Docs](#) › [Elastic Security Solution \[8.15\]](#) › [Detections and alerts](#)
› [Prebuilt rule reference](#)

Microsoft IIS Service Account Password Dumped



Identifies the Internet Information Services (IIS) command-line tool, AppCmd, being used to list passwords. An attacker with IIS web server access via a web shell can decrypt and dump the IIS AppPool service account password using AppCmd.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.process-*
- logs-windows.*
- endgame-*
- logs-system.security*

Severity: low

Risk score: 21

Runs every: 5m

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

Maximum alerts per execution: 100

References:

- <https://blog.netspi.com/decrypting-iis-passwords-to-break-out-of-the-dmz-part-1/>

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Credential Access
- Data Source: Elastic Endgame
- Data Source: Elastic Defend
- Rule Type: BBR
- Data Source: System

Version: 214

Rule authors:

- Elastic

Rule license: Elastic License v2

Rule query



```
process where host.os.type == "windows" and event.type  
  (process.name : "appcmd.exe" or ?process.pe.original_name  
    process.args : "list" and process.args : "/text*")
```

Framework: MITRE ATT&CK™

- Tactic:
 - Name: Credential Access

- ID: TA0006
- Reference URL:
<https://attack.mitre.org/tactics/TA0006/>
- Technique:
 - Name: OS Credential Dumping
 - ID: T1003
 - Reference URL:
<https://attack.mitre.org/techniques/T1003/>

« [Microsoft IIS Connection Strings Decryption](#)

[Microsoft Management Console File from Unusual Path](#) »

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

in



f



• 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.