

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).  
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Learn more and customize

Reject

Accept

# 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

ElasticON events are back!  
Learn about the Elastic Search AI Platform from the experts at our live events.

Learn more

Was this helpful?



Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).  
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

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](#) »



Follow us



About us

- About Elastic
- Leadership
- DE&I
- Blog
- Newsroom

Join us

- Careers
- Career portal

Investor relations

- Investor resources
- Governance
- Financials
- Stock

Partners

- Find a partner
- Partner login
- Request access
- Become a partner

Trust & Security

- Trust center
- EthicsPoint portal
- ECCN report
- Ethics email

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the [cookie policy](#).  
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.