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-thedmz-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 Al
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&CKTM

- 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 »



The Search Al 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

Microsoft IIS Service Account Password Dumped | Elastic Security Solution [8.15] | Elastic - 02/11/2024 15:40 https://www.elastic.co/guide/en/security/current/microsoft-iis-service-account-password-dumped.html

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.

<u>Trademarks</u> <u>Terms of Use</u> <u>Privacy</u> <u>Sitemap</u> © 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.