

Q

8

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 Connection Strings Decryption



Identifies use of aspnet_regiis to decrypt Microsoft IIS connection strings. An attacker with Microsoft IIS web server access via a webshell or alike can decrypt and dump any hardcoded connection strings, such as the MSSQL service account password using aspnet_regiis command.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.process-*
- logs-windows.forwarded*
- logs-windows.sysmon_operational-*
- endgame-*
- logs-system.security*
- logs-m365_defender.event-*
- logs-sentinel_one_cloud_funnel.*

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: 33

References:

- https://blog.netspi.com/decrypting-iis-passwords-tobreak-out-of-the-dmz-part-1/
- https://symantec-enterpriseblogs.security.com/blogs/threat-intelligence/greenbugespionage-telco-south-asia

Tags:

Domain: Endpoint

OS: Windows

Use Case: Threat Detection

Tactic: Credential Access

• Data Source: Elastic Endgame

• Data Source: Elastic Defend

• Data Source: System

• Data Source: Microsoft Defender for Endpoint

• Data Source: Sysmon

• Data Source: SentinelOne

Version: 311

Rule authors:

Elastic

Rule license: Elastic License v2

Rule query



```
process where host.os.type == "windows" and eventaty
  (process.name : "aspnet_regiis.exe" or ?process.pe
  process.args : "connectionStrings" and process.arg
```

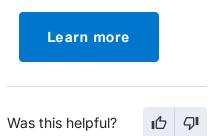
Framework: MITRE ATT&CKTM

- 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 Exchange Worker Spawning Suspicious Processes Microsoft IIS Service Account
Password Dumped »

ElasticON events are back!

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





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

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events

Microsoft IIS Connection Strings Decryption | Elastic Security Solution [8.15] | Elastic - 31/10/2024 18:16 https://www.elastic.co/guide/en/security/current/microsoft-iis-connection-strings-decryption.html

<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.