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

edit

```
process where host.os.type == "windows" and event.ty
  (process.name : "appcmd.exe" or ?process.pe.origi
  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 »