Elastic Security:

8.15 (current)

Elastic Security overview

What's new in 8.15

Upgrade Elastic Security to 8.15.3

Post-upgrade steps (optional)

Get started with Elastic Security

AI for security

Detections and alerts

- Detections prerequisites and requirements
- About detection rules
- Create a detection rule
- Install and manage Elastic prebuilt rules
- Manage detection rules
- Monitor and troubleshoot rule executions
- Rule exceptions
- About building block rules

Unusual File Modification by dns.exe

Identifies an unexpected file being modified by dns.exe, the process responsible for Windows DNS Server services, which may indicate activity related to remote code execution or other forms of exploitation.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.file-*
- logs-windows.sysmon_operational-*
- endgame-*

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: 100

MITRE ATT&CK® coverage

Manage detection alerts ›

References:

- https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
- https://msrc-blog.microsoft.com/2020/07/14/july-2020-security-update-cve-2020-1350-vulnerability-in-windows-domain-name-system-dns-server/
- https://www.elastic.co/security-labs/detection-rules-for-sigred-vulnerability

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Lateral Movement
- Data Source: Elastic Endgame
- Use Case: Vulnerability
- Data Source: Elastic Defend
- Data Source: Sysmon

Version: 211

Rule authors:

- Elastic

Rule license: Elastic License v2

Investigation guide

edit

Triage and analysis

Investigating Unusual File Write

Detection alerts from this rule indicate potential unusual/abnormal file writes from the DNS Server service process (`dns.exe`) after exploitation from CVE-2020-1350 (SigRed) has occurred. Here are some possible avenues of investigation: - Post-exploitation, adversaries may write additional files or payloads to the system as additional discovery/exploitation/persistence mechanisms. - Any suspicious or abnormal files written from `dns.exe` should be reviewed and investigated with care.

Rule query

edit

```
file where host.os.type == "windows" and process.nam
  not file.name : "dns.log" and not
  (file.extension : ("old", "temp", "bak", "dns", "a

  /* DNS logs with custom names, header converts to
  not ?file.Ext.header_bytes : "444e5320536572766572
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Lateral Movement
  - ID: TA0008
  - Reference URL: https://attack.mitre.org/tactics/TA0008/
- Technique:
  - Name: Exploitation of Remote Services
  - ID: T1210
  - Reference URL: https://attack.mitre.org/techniques/T1210/

« Unusual File Creation - Alternate Data Stream

Unusual High Confidence Misconduct Blocks Detected »