

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

WebServer Access Logs Deleted

edit

Identifies the deletion of WebServer access logs. This may indicate an attempt to evade detection or destroy forensic evidence on a system.

Rule type: eql

Rule indices:

- auditbeat-*
- winlogbeat-*
- logs-endpoint.events.*
- logs-windows.sysmon_operational-*

Severity: medium

Risk score: 47

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also

Additional look-back time

Maximum alerts per execution: 100

References: None

Tags:

Domain: Endpoint

• OS: Linux

OS: Windows

OS: macOS

Use Case: Threat Detection

• Tactic: Defense Evasion

• Data Source: Elastic Defend

• Data Source: Sysmon

Version: 207

Rule authors:

Elastic

Rule license: Elastic License v2

Setup



Setup

If enabling an EQL rule on a non-elastic-agent index (such as beats) for versions <8.2, events will not define event.ingested and default fallback for EQL rules was not added until version 8.2. Hence for this rule to work effectively, users will need to add a custom ingest pipeline to populate event.ingested to @timestamp. For more details on adding a custom ingest pipeline refer - https://www.elastic.co/guide/en/fleet/current/data-streams-pipeline-tutorial.html

Rule query



Framework: MITRE ATT&CKTM

- Tactic:
 - Name: Defense Evasion
 - ID: TA0005
 - Reference URL: https://attack.mitre.org/tactics/TA0005/
- Technique:
 - Name: Indicator Removal
 - ID: T1070
 - Reference URL: https://attack.mitre.org/techniques/T1070/

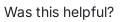
« WebProxy Settings Modification

Werfault ReflectDebugger
Persistence »

ElasticON events are back!

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

Learn more









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

https://www.elastic.co/guide/en/security/current/webserver-access-logs-deleted.html

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events

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

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.