

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

# UAC Bypass via ICMLuaUtil Elevated COM Interface



Identifies User Account Control (UAC) bypass attempts via the ICMLuaUtil Elevated COM interface. Attackers may attempt to bypass UAC to stealthily execute code with elevated permissions.

Rule type: eql

#### Rule indices:

- winlogbeat-\*
- logs-endpoint.events.process-\*
- logs-windows.sysmon\_operational-\*
- endgame-\*
- logs-m365\_defender.event-\*

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

References: None

#### Tags:

• Domain: Endpoint

OS: Windows

• Use Case: Threat Detection

• Tactic: Privilege Escalation

• Tactic: Defense Evasion

• Tactic: Execution

• Data Source: Elastic Endgame

• Data Source: Elastic Defend

• Data Source: Sysmon

Data Source: Microsoft Defender for Endpoint

Version: 210

#### Rule authors:

Elastic

Rule license: Elastic License v2

### Rule query



process where host.os.type == "windows" and eventity
process.parent.name == "dllhost.exe" and
process.parent.args in ("/Processid:{3E5FC7F9-9A51-process.pe.original\_file\_name != "WerFault.exe"

Framework: MITRE ATT&CK<sup>TM</sup>

Tactic:

- Name: Privilege Escalation
- ID: TA0004
- Reference URL: https://attack.mitre.org/tactics/TA0004/
- Technique:
  - Name: Abuse Elevation Control Mechanism
  - ID: T1548
  - Reference URL: https://attack.mitre.org/techniques/T1548/
- Sub-technique:
  - Name: Bypass User Account Control
  - ID: T1548.002
  - Reference URL: https://attack.mitre.org/techniques/T1548/002/
- Tactic:
  - Name: Defense Evasion
  - ID: TA0005
  - Reference URL: https://attack.mitre.org/tactics/TA0005/
- Technique:
  - Name: Abuse Elevation Control Mechanism
  - ID: T1548
  - Reference URL: https://attack.mitre.org/techniques/T1548/
- Sub-technique:
  - Name: Bypass User Account Control
  - ID: T1548.002
  - Reference URL: https://attack.mitre.org/techniques/T1548/002/

• Tactic:

• Name: Execution

• ID: TA0002

 Reference URL: https://attack.mitre.org/tactics/TA0002/

• Technique:

Name: Inter-Process Communication

• ID: T1559

 Reference URL: https://attack.mitre.org/techniques/T1559/

• Sub-technique:

• Name: Component Object Model

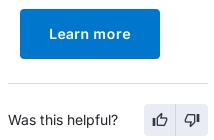
• ID: T1559.001

 Reference URL: https://attack.mitre.org/techniques/T1559/001/

« UAC Bypass via DiskCleanup Scheduled Task Hijack UAC Bypass via Windows Firewall Snap-In Hijack »

#### 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

**UAC Bypass via ICMLuaUtil Elevated COM Interface | Elastic Security Solution [8.15] | Elastic -** 31/10/2024 19:41 https://www.elastic.co/guide/en/security/current/uac-bypass-via-icmluautil-elevated-com-interface.html

## Investor relations

Investor resources

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>

© 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.