UAC Bypass via ICMLuaUtil Elevated COM Interface

edit

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

Was this helpful?

Framework: MITRE ATT&CK^{TM}

- 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/