



Official Incident Report

Date: Jun, 21, 2023, 11:02 AM

Event ID: 161

Rule Name: SOC211 - Utilman.exe Winlogon Exploit Attempt

Table of Contents

Alert Details..... 2

Detection 3

Verify.....4

Analysis.....4

Containment 10

Summary..... 11

Lessons Learned 12

Remediation Actions 13

Appendix 13

MITRE ATT&CK 14

Artifacts 14

LetsDefend Playbook..... 14

Alert Details

Severity: Medium

Type: LOLBin

Hostname: Henry

Ip Address: 172.16.17.149

Process Name: Utilman.exe

Process Hash: ded8fd7f36417f66eb6ada10e0c0d7c0022986e9

Parent Process: Winlogon.exe

Command Line: net user superman onepunch123 /add

Trigger Reason: Command Launched from Winlogon

Device Action: Allowed

Based on the information provided in the alert, it appears that an attacker has executed a **living-off-the-land binary**, running on **Henry** host **172.16.17.149**. The alert is triggered by rule SOC211 - Utilman.exe Winlogon Exploit Attempt.

It is important to check what commands were run using the **utilman.exe** binary. The device action is marked **allowed**, indicating that the binary was successfully executed.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

According to [Talos Intelligence](#), a LoLBin is any binary supplied by the operating system that is normally used for legitimate purposes but can also be abused by malicious actors. Several default system binaries have unexpected side effects, which may allow attackers to hide their activities post-exploitation.

The **utilman.exe** binary has a vulnerability where an attacker can rename **utilman.exe** to something else and **cmd.exe** to **utilman.exe** and use this to bypass the windows password.

Analysis

The next step of our investigation into this potential **LOLBin** attack is to search for any emails notifying of any potential pentesting, however, **no emails** were found. This alert could either be a **false positive**, where an internal pentester is searching for vulnerabilities, or a **true positive** where an attacker is searching for vulnerabilities.

To investigate this alert, we must search through Endpoint Security, specifically **Henry**.

Host Information			
Hostname:	Henry	Domain:	LetsDefend
IP Address:	172.16.17.149	Bit Level:	64
OS:	Windows 10	Primary User:	Henry
Client/Server:	Client	Last Login:	Jun, 21, 2023, 12:24 PM

Furthermore, we can investigate the device's Terminal History.

EVENT TIME	COMMAND LINE
2023-06-21 10:06:34.82	cd C:\Windows\System32
2023-06-21 10:07:05.123	rename utilman.exe utilman.old
2023-06-21 10:07:12.580	copy cmd.exe utilman.exe
2023-06-21 10:24:08.809	shutdown /h /t 0
2023-06-21 11:00:00.743	net user
2023-06-21 11:00:09.520	whoami
2023-06-21 11:02:12.657	net user superman onepunch123 /add
2023-06-21 11:03:14.706	net localgroup administrators superman /add

The first command **cd C:\Windows\System32** moves into System32 directory where critical executables live.

The second command **rename utilman.exe utilman.old**, Utilman.exe is legitimate and responsible for launching the Ease of Access Center on Windows login screen for accessibility features. The command renames the original utilman.exe file, moving it so that it can be replaced in future by an executable file of the attacker's choice. This is a preparation step to replace utilman.exe with cmd.exe, so that a cmd prompt can appear at the login screen

The third command **copy cmd.exe utilman.exe** copies cmd.exe to utilman.exe, replacing the Ease of Access executable with a command shell. Now, when clicking the Ease of Access button on the login screen, instead of launching utilman.exe, cmd.exe will launch a SYSTEM-level command prompt to appear instead of the accessibility features

The fourth command **shutdown /h /t 0** immediately shuts down the system to finalize changes.

The fifth command **net user** checked local users.

The sixth command **whoami** checked the account context of who they were running under.

The seventh command **net user superman onepunch123 /add** creates a new user “superman” with password “onepunch123”.

The eighth command **net localgroup administrators superman /add** adds user “superman” to the local administrators group. It escalates the new users' privileges (user account elevation).

Based on these commands, the operator created a **privileged account** and installed a reliable method to launch a SYSTEM-level **shell** at the **login screen**. This combination enables easy re-entry and full system control without normal authentication.

After we confirm the attack via Endpoint Security, we can analyse the logs of the incident.

Field	Value
type	Proxy
source_address	93.184.220.29
source_port	80
destination_address	172.16.17.149
destination_port	18496
time	May, 15, 2023, 02:40 AM

<https://www.virustotal.com/gui/ip-address/93.184.220.29>

1/95 security vendor flagged this IP address as malicious


<https://www.abuseipdb.com/check/93.184.220.29>

93.184.220.29 was found in our database!

This IP was reported **160** times. Confidence of Abuse is **0%**:

?

0%

ISP	NETBLK-03-EU-93-184-220-0-22
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Domain Name	edg.io
Country	 United States of America
City	El Segundo, California

Field	Value
type	Firewall
source_address	76.13.32.141
source_port	443
destination_address	172.16.17.149
destination_port	33166
time	May, 02, 2023, 12:57 PM

<https://www.virustotal.com/gui/ip-address/76.13.32.141>

4 detected files communicating with this IP address

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required.

Host Information				Action	
Hostname:	Henry	Domain:	LetsDefend	Containment:	<input checked="" type="checkbox"/> Host Contained
IP Address:	172.16.17.149	Bit Level:	64		
OS:	Windows 10	Primary User:	Henry		
Client/Server:	Client	Last Login:	Jun, 21, 2023, 12:24 PM		

Summary

The incident involves a compromised system named **Henry** with an IP address of **172.16.17.149**. The alert was triggered by the detection of a potential **LOLBin** attack via the **utilman.exe** binary, based on the rule **SOC211 - Utilman.exe Winlogon Exploit Attempt**.

The attacker has replaced the **utilman.exe** file with a **cmd.exe**, making it so when the user clicks on the **Ease of Access** button on the **windows login screen**, a SYSTEM-level **shell prompt appears**, allowing the user to **create a local account**, and **elevate it's privileges** to become a **local administrator**. This gives an attacker a **backdoored admin account** without normal authentication (Persistence & Privilege-Escalation).

Immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- Critical Windows system files must be protected and audited, as they are common privilege-escalation targets
- Local console access, privileged accounts, or offline boot methods may not be tightly controlled, and winlogon-related activity needs better visibility
- Local admin or system-level access must be more tightly restricted and audited

Remediation Actions

- Reinstall or restore utilman.exe and any other modified Windows binaries
- Harden local access & physical security, and restrict administrative privileges
- Whitelist approved admin tools and maintained a list of legitimate uses of LOLBins

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1078 - Valid Accounts
Persistence	T1546.008 - Event Triggered Execution: Accessibility Features
Privilege Escalation	T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control

Artifacts

Value	Comment	Type
93.184.220.29	Malicious communication	IP Address
76.13.32.141	Malicious communication	IP Address
ded8fd7f36417f66eb6ada10e0c0d7c0022986e9	Winlogon.exe	MD5 Hash

LetsDefend Playbook

[LetsDefend Event ID: 161](#)