



# Detecting Privilege Escalation Zero Day (CVE-2021-41379)

November 24th, 2021 - 3 min read

by Bhabesh Raj Rai, Associate Security Analytics Engineer

On November 22, 2021, Security researcher [Abdelhamid Naceri](#) dropped PoC for a privilege escalation vulnerability (CVE-2021-41379) in the Windows installer that Microsoft had patched in November's Patch Tuesday. The PoC works on all supported versions of Windows.

The specific flaw exists within the Windows Installer service. An attacker can abuse the Windows Installer service to delete a file or directory by creating a junction. Instead of providing the bypass, Naceri provided a more powerful variant of the vulnerability that allows an unprivileged user to run the command prompt as SYSTEM.

Naceri explained that his PoC would bypass any group policies configured to prevent normal users from performing MSI installations.

## Detecting Exploitation in LogPoint

A naive detection approach for exploitation of this zero-day is via Application installation logs. Look out for the application name "test pkg" used in the PoC.

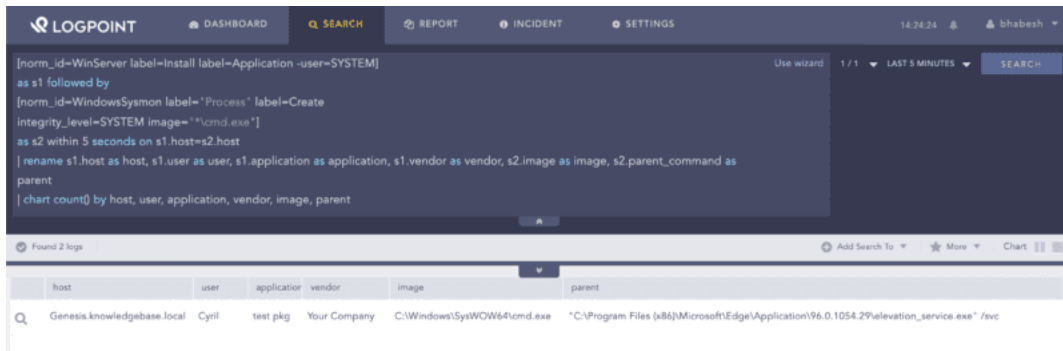
```
norm_id=WinServer label=Application label=Install application="test pkg"
```

Threat actors can change the PoC defaults for stealth. We can use process creation logs that can catch this configuration change. Look out for spawning of x32 command prompt by Microsoft Edge Elevation Service.

```
norm_id=WindowsSysmon label="Process" label=Create  
integrity_level=SYSTEM image="*\cmd.exe"  
parent_command='*\elevation_service.exe' /svc'  
image="C:\Windows\SysWOW64\cmd.exe"
```

Finally, we present a generic detection approach that looks for execution of elevated command prompt preceded by application installation within 5 seconds.

```
[norm_id=WinServer label=Install label=Application -user=SYSTEM]  
as s1 followed by  
[norm_id=WindowsSysmon label="Process" label=Create  
integrity_level=SYSTEM image="*\cmd.exe"]  
as s2 within 5 seconds on s1.host=s2.host  
| rename s1.host as host, s1.user as user, s1.application as application,  
s1.vendor as vendor, s2.image as image, s2.parent_command as parent  
| chart count() by host, user, application, vendor, image, parent
```



## Monitor for exploitation attempt

According to Naceri, the best workaround available is to wait for Microsoft's patch. In the meantime, we recommend that enterprise defenders monitor for any exploitation attempt of this critical local privilege escalation (LPE) zero-day. As the PoC is public, we can expect ransomware and less sophisticated threat actors to add this in their arsenal to decrease their time to objective metric

## Discover More About Logpoint

[Book a demo](#)[Customer cases](#)[Customer reviews](#)

### Related Posts



#### Uncover more resources with Logpoint's latest release

October 30th, 2024



#### Latrodectus: The Wrath of Black Widow

October 22nd, 2024



Detect. Manage. Respond.

Products

- SIEM
- Automation
- Case Management
- Behavior Analytics
- Cyber Defense Platform
- Pricing
- Sizing Calculator

Why Logpoint?

- Product Recognition
- Customer Cases
- EAL3+ Certificate
- Newsletter



Company

- About us
- Management
- Careers at Logpoint
- Media Room
- Logpoint in the media
- Blog & Webinars

Support

- Cyber Library
- Service Desk
- Documentation
- Community
- Contact
- Status

Contact

-  [info@logpoint.com](mailto:info@logpoint.com)
-  +45 7060 6100
- 