



PRIVACY

WHO WE ARE

HOW IT WORKS

BLOG

ADVISORIES

LOG IN | SIGN UP

# ADVISORY DETAILS

November 11th, 2021

## Microsoft Windows Installer Service Link Following Privilege Escalation Vulnerability

ZDI-21-1308  
ZDI-CAN-14616

CVE ID	CVE-2021-41379
CVSS SCORE	7.8, AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
AFFECTED VENDORS	Microsoft
AFFECTED PRODUCTS	Windows
VULNERABILITY DETAILS	<p>This vulnerability allows local attackers to escalate privileges on affected installations of Microsoft Windows. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.</p> <p>The specific flaw exists within the Windows Installer service. By creating a junction, an attacker can abuse the service to delete a file or directory. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM.</p>
ADDITIONAL DETAILS	Microsoft has issued an update to correct this vulnerability. More details can be found at: <a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379</a>
DISCLOSURE TIMELINE	2021-08-10 - Vulnerability reported to vendor 2021-11-11 - Coordinated public release of advisory
CREDIT	Abdelhamid Naceri

< BACK TO ADVISORIES



Find us on Mastodon

[Mastodon](#)

Media Inquiries

[media\\_relations@trendmicro.com](mailto:media_relations@trendmicro.com)

Sensitive Email Communications

[PGP Key](#)

WHO WE ARE

- [Our Mission](#)
- [Trend Micro](#)
- [TippingPoint IPS](#)

HOW IT WORKS

- [Process](#)
- [Researcher Rewards](#)
- [FAQS](#)
- [Privacy](#)

ADVISORIES

- [Published Advisories](#)
- [Upcoming Advisories](#)
- [RSS Feeds](#)

BLOG

