by **Evan Schuman**
Contributor

Updated

Researcher bypasses Microsoft Defender security patch, seizing control

News
Aug 12, 2026 • 6 mins

The PoC posted by Nightmare Eclipse, who has been feuding with Microsoft for months, enables an attacker with any level of access to gain system-level privileges.

Credit: Mats Wiklund / Shutterstock

Just weeks after Microsoft patched a critical hole in Microsoft Defender, a cybersecurity researcher has posted an apparent bypass that provides system-level control to attackers once they gain any level of access.

The researcher, who goes by the name Nightmare Eclipse, has been engaged in a **long-running battle with Microsoft Security [https://www.csoonline.com/article/4178869/microsoft-and-security-researchers-dueling-posts-about-cybersecurity-disclosures-get-nasty.html]**.

Nightmare Eclipse has not provided the further details we requested, however Microsoft sent a brief statement, saying, "Microsoft is aware of the reported vulnerability and is actively investigating the validity and potential applicability of these claims," and reiterating its commitment to investigating issues and supporting coordinated disclosure.
But the proof of concept (PoC) security bypass, ShieldBreak, **described by Nightmare Eclipse [https://github.com/MSNightmare/ShieldBreak]** in **a series of [https://git.projectnightcrawler.dev/NightmareEclipse/ShieldBreak]** public **posts [https://git.churchofmalware.org/Nightmare_Eclipse/ShieldBreak]**, potentially threatens to be more damaging than earlier bypass.

Like other **recently reported vulnerabilities [https://www.csoonline.com/article/4205751/enterprise-passkey-security-under-threat-from-malware-2.html]**, ShieldBreak requires an attacker to first somehow gain system access, typically via a successful phishing scam. Once in, however, the attacker can gain full admin/root access.

But there is a troubling psychological component to ShieldBreak, in that it is a bypass for a recently posted security patch from Microsoft, noted **Justin Greis [https://acceligence.com/talent/profiles/justin-greis/]**, CEO of consulting firm Acceligence. The problem is that CISOs who have already deployed that patch might feel protected when they are not.

Recommended for you

Another Microsoft Defender privilege escalation bug emerges days after patch

By Shweta Sharma • 3 mins

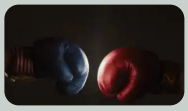
[https://www.csoonline.com/?post_type=post&p=4160275&utm_source=miso&utm_medium=related&utm_campaign=thumbnail_list]

Windows Defender's own

[https://www.csoonline.com/?post_type=post&p=42129

driver can leave systems defenseless
By Shweta Sharma • 4 mins

29&utm_source=miso&utm_medium=related&utm_campaign=thumbnail_list]



Microsoft feud escalates as researcher drops new Windows zero-day
By Shweta Sharma • 4 mins

[https://www.csoonline.com/?post_type=post&p=4183487&utm_source=miso&utm_medium=related&utm_campaign=thumbnail_list]

“This one is concerning because the patch bypass directly calls the integrity of the remediation into question,” he said. “ShieldBreak appears to demonstrate that an attacker can bypass the fix Microsoft shipped for CVE-2026-50656 and ultimately obtain system-level privileges on the endpoint. That is an important distinction for enterprise defenders, because organizations may believe they have already remediated the underlying vulnerability. A successful patch bypass means the exposure can persist even after the normal vulnerability-management process says the system is protected.”

Greis added that such bypass can reduce overall trust in official patches.

“When public proof of concept code can bypass it, the CISO’s question becomes ‘have we actually removed the exposure?’ rather than simply ‘have we deployed the patch?’,” he said. “From an architecture perspective, organizations should be very careful about allowing the same security product to become both the control being relied upon and the only source of evidence that the control is working.”
Flavio Villanustre [https://www.linkedin.com/in/fvillanustre/], CISO for the LexisNexis Risk Solutions Group, said he was especially concerned about the timing of the PoC’s release, given that it seemed to be intended to put the most pressure on Microsoft, given its **typical timing for security patches** [https://www.csoonline.com/article/4208185/patch-tuesday-august-2026-a-zero-day-winsock-driver-hole-under-exploit-and-a-maximum-severity-sap-vulnerability.html].

- Is the BlueHammer zero-day exploit linked to recent Defender privilege escalations?
- How are attackers exploiting the critical Microsoft WSUS deserialization flaw?
- Can the Cloud Files API be used to gain SYSTEM-level access?

Ask a question

Ask

"This vulnerability, if valid, would need a fix from Microsoft, but because those patches are usually only released on the second Tuesday of the month and the security researcher seems to have carefully timed the release of the PoC, we may have this exposure for another 4 weeks unless Microsoft deems this a very high severity risk, which is unlikely," he pointed out.

Cybersecurity consultant **Brian Levine** [https://formergov.com/directory/brianlevine], executive director of FormerGov, agreed that CISOs should not underestimate the damage potential if this PoC proves valid.

"What makes it dangerous is what it does once they're in: it turns an ordinary low-privilege account into full system control by abusing Defender itself, the security tool running at the highest privilege on the box," he said. "An exploit that lives inside your antivirus is quiet, it's trusted, and it can be used to blind or disable the very thing you're counting on to catch the intruder. It's not a worm, but it's a near-ideal second stage for ransomware crews and anyone doing hands-on-keyboard intrusion."

Levine suggested that CISOs not wait for a Microsoft fix, but immediately take an aggressive defensive stance.

"Assume it's live and lean on defense in depth, because this is exactly the scenario where treating Defender as your only line fails you. Application allowlisting, such as WDAC or AppLocker in enforced mode, is the strongest hardening available and can stop the payload even if the race succeeds," Levine said.
"Tighten local admin rights and least privilege so a foothold has less to escalate from. And give your hunters one very specific thing to watch for: an interactive shell or scripting host running as system whose parent process is Defender's engine, MsMpEng.exe. That should never happen in a healthy environment and it's a high-fidelity sign someone is running this."

But he also suggested that CISOs not assume that the PoC necessarily works as advertised.

“This is a single researcher’s proof of concept. It hasn’t been independently verified, and it’s coming from someone in the middle of a very public and very bitter fight with Microsoft, so perhaps some of the theater around it should be discounted,” Levine said. “But you can’t wave it away either. Patch bypasses are extremely common, and the claim that Microsoft’s fix for RoguePlanet didn’t fully close the door is entirely plausible. Defenders should treat it as credible until proven otherwise, not the reverse.”
Although Levine and other analysts were initially dubious, there are now indications that the PoC’s effectiveness has been independently verified.

Cybersecurity and risk advisor **Steven Eric Fisher** [https://www.linkedin.com/in/stevenericc/], a former cybersecurity risk specialist at Walmart, said, “I’ve seen **independent confirmation** [https://cyberplace.social/@GossiTheDog/117082623896479140] that ShieldBreak works, although its exploitation method differs materially from the original RoguePlanet exploit. RoguePlanet relied on a filesystem race condition, while ShieldBreak appears to use a different Defender/Cloud Filter API path,” Fisher said. “So while it is being characterized as a bypass of Microsoft’s CVE-2026-50656 fix, it is not simply a replay of the original exploit.”

He added that cybersecurity researcher Kevin Beaumont has already published **Microsoft Defender Advanced Hunting detections** [https://github.com/GossiTheDog/ThreatHunting/blob/master/AdvancedHuntingQueries/ShieldBreak.kql] for ShieldBreak that organizations can incorporate into monitoring while evaluating their exposure.
And **Pieter Arntz** [https://www.linkedin.com/in/pieter-arntz-04164b2/], malware intelligence researcher at Malwarebytes, also said he has seen confirmation from a researcher he tracks, **Will Dormann** [http://and%20peter%20arntz,%20malware%20intelligence%20researcher%20at%20malwarebytes,%20said%20he%20has%20seen%20confirmation%20from%20a%20researcher%20he%20tracks%20named%20will%20dormann.https//infosec.exchange/@wdormann/117079587486018149].

This article has been updated with a statement from Microsoft and further confirmation of the exploit.

Vulnerabilities[https://www.csoonline.com/vulnerabilities/] Security[https://www.csoonline.com/security/]

Hacking[https://www.csoonline.com/hacking/] Cybercrime[https://www.csoonline.com/cybercrime/]

Join the CSO First Look mailing list for the latest news, analysis, and insights. Sign up now!

Email Address

By submitting your information, you agree to our PRIVACY POLICY [https://foundryco.com/privacy-policy/].

Subscribe

About

- About Us
- Advertise
- Contact Us
- Editorial ethics policy
- Foundry Careers
- Reprints
- Newsletters
- Contribute to CSO
- Add CSO as a Preferred Source in Google Search

Policies

- Terms of Service
- Privacy Policy
- Cookie Policy
- Copyright Notice
- Member Preferences
- About AdChoices
- Your California Privacy Rights

More

- Awards
- Blogs
- BrandPosts
- Events
- Podcasts

Our Network

- CIO
- Computerworld
- InfoWorld
- Network World

FOUNDRY