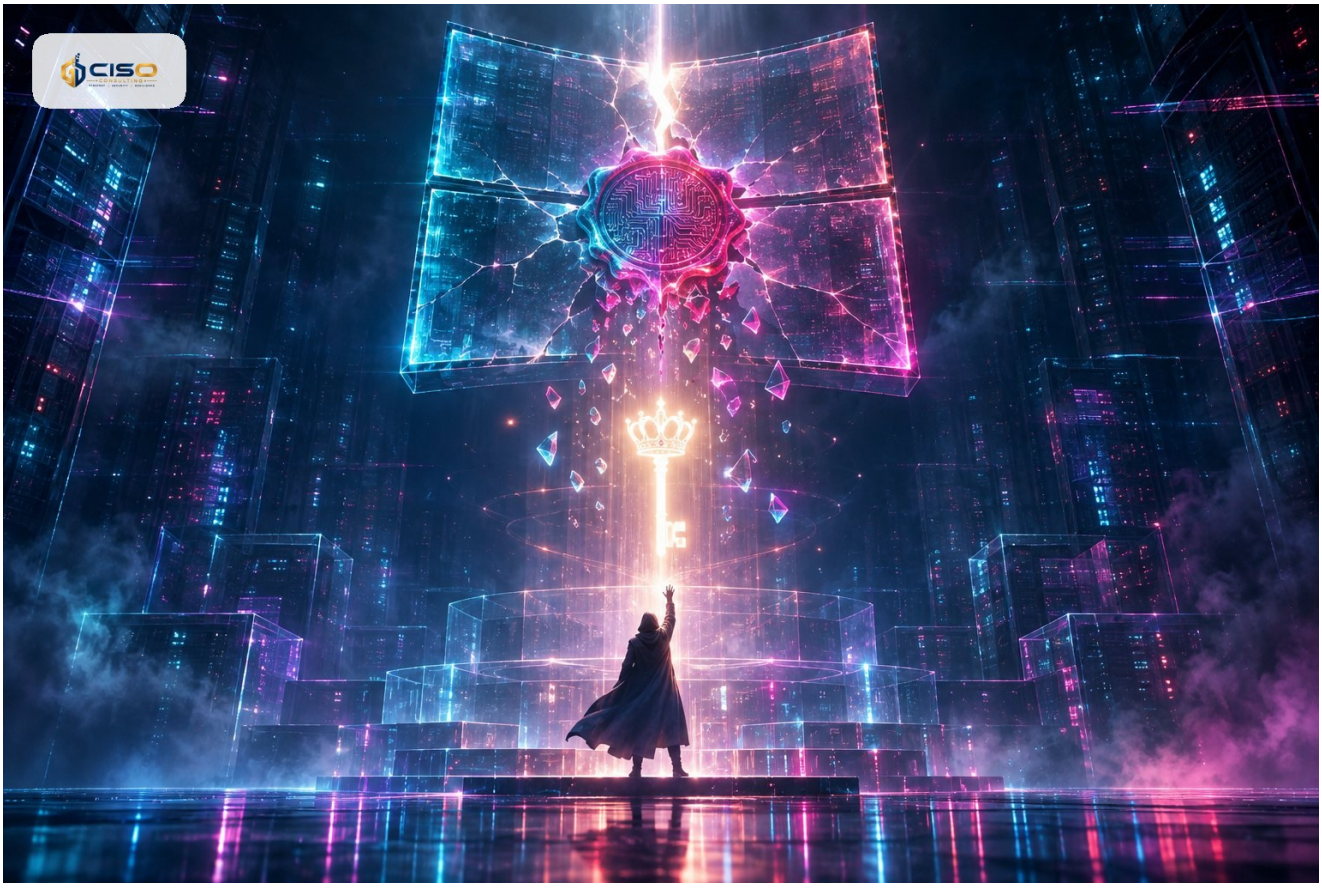
SignDrop: New Windows Zero-Day Exploit Released, Enabling SYSTEM Privileges



A researcher known as Nightmare Eclipse has released an exploit for a new Windows zero-day, called SignDrop, that can give attackers SYSTEM privileges. The source provides few further details.

- Researcher Abdelhamid Naceri, also known as Nightmare Eclipse, has published a new Windows zero-day exploit.
- The flaw is referred to as SignDrop.
- Successful exploitation can let an attacker obtain SYSTEM privileges, the highest level on a Windows host.
- The available text does not mention a CVE number, a patch or confirmed attacks.

What has been reported

Security researcher Abdelhamid Naceri, who also uses the name Nightmare Eclipse, has released an exploit for a previously unknown Windows vulnerability named **SignDrop**. According to the report, the exploit can allow an attacker to gain SYSTEM privileges.

A zero-day is a flaw for which no fix was available when details became public. The portion of the article available to us does not state a CVE identifier, which Windows versions are affected, whether Microsoft has responded, or whether the flaw is being used in real attacks.

Why it matters

SYSTEM is the highest privilege level on a Windows machine. A local privilege escalation of this kind is typically used after an attacker already has a foothold, for example through a stolen low-privilege account or malware running as a normal user. With SYSTEM rights, an attacker could disable security tools or reach credentials. Publication of exploit code can also shorten the time before others reuse it.

What to do now

Treat this as a developing issue. Until the vendor publishes guidance, the practical priority is to limit the chance that an attacker gains an initial foothold and to improve the ability to detect privilege escalation. Confirm the status with official Microsoft channels before taking any change-heavy steps, and avoid running unverified exploit code in production environments.

What to do now

1. Monitor official Microsoft channels for an advisory, CVE assignment and patch for SignDrop.
2. Review and reduce local administrator rights and low-privilege accounts on Windows endpoints and servers.
3. Ensure EDR and logging can alert on unusual privilege escalation to SYSTEM and on tampering with security tools.
4. Prioritise controls against initial access, such as phishing protection and application allow-listing, on critical systems.
5. Do not test public exploit code on production systems; use isolated lab environments if validation is needed.