Microsoft Windows Zero-Day Exploits - YellowKey BitLocker Bypass and GreenPlasma Privilege Escalation

TL;DR

A security researcher known as "Chaotic Eclipse" or "Nightmare Eclipse" released proof-of-concept (PoC) code for two new Microsoft Windows zero-days named YellowKey and GreenPlasma. The same researcher was previously tied to the public disclosure of the BlueHammer and RedSun vulnerabilities.

YellowKey is a BitLocker bypass affecting TPM-only systems. GreenPlasma is a local privilege escalation flaw tied to the Windows CTFMON process. Public exploit code and growing attention around these flaws increase the likelihood of copycat activity.

Overview

A security researcher known as "Chaotic Eclipse" or "Nightmare Eclipse," previously tied to the BlueHammer and RedSun zero-days, released two new Windows vulnerabilities named YellowKey and GreenPlasma. Public proof-of-concept (PoC) code is available for both vulnerabilities. At this time, neither vulnerability has an assigned CVE identifier or official Microsoft advisory.

YellowKey is a BitLocker bypass affecting Windows 11 and Windows Server 2022/2025 systems using TPM-only BitLocker. The exploit abuses the Windows Recovery Environment (WinRE) to access unlocked drives without credentials. If exploited, an attacker with physical access to the device may be able to access sensitive files, steal data, or bypass disk encryption protections. It has been confirmed that the exploit works against TPM-only configurations.

GreenPlasma is a local privilege escalation vulnerability tied to the Windows CTFMON process. The flaw may allow a low-privileged user to gain SYSTEM-level access. If exploited, an attacker may be able to take control of the affected system, execute commands with elevated privileges, or interfere with trusted services and drivers.

The researcher also claimed Microsoft silently patched another vulnerability called RedSun without assigning a CVE or publishing an advisory. According to current public reporting, Microsoft has not formally acknowledged YellowKey or GreenPlasma, which is likely why CVE identifiers have not been assigned. Organizations using TPM-only BitLocker should review systems that rely on automatic disk unlock functionality.

Aspire Protects

- **Patch** - Microsoft has not issued a formal security advisory or publicly confirmed YellowKey or GreenPlasma at this time. The vulnerabilities are currently only being discussed through public researcher disclosures and third-party reporting. Until Microsoft issues a patch, please see the recommendations below:
    - Configure BitLocker to require TPM+PIN instead of TPM-only authentication where operationally possible.
    - Set BIOS/UEFI passwords on company systems to reduce unauthorized boot modifications.
    - Restrict booting from external USB devices in BIOS/UEFI settings.
    - Monitor systems for unexpected WinRE activity or unauthorized recovery environment launches.
    - Monitor for suspicious modification of EFI partitions or FsTx-related files.
    - Limit local administrator access and enforce least privilege controls.
    - Watch for abnormal behavior involving ctfmon.exe and SYSTEM-level object creation.
    - Monitor Microsoft Security Response Center (MSRC) advisories for future guidance related to YellowKey or GreenPlasma.

TTPs to Watch

Defense Evasion

- Subvert Trust Controls [T1553] – The attacker may abuse trusted Windows Recovery Environment (WinRE) functionality and BitLocker auto-unlock behavior to bypass disk encryption protections. (YellowKey)

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may exploit GreenPlasma to elevate privileges from a standard user account to SYSTEM-level access. (GreenPlasma)

IoCs

Files / Artifacts

- FsTx transaction files associated with WinRE exploitation
- Unexpected modification of winpeshl.ini

- Suspicious activity involving ctfmon.exe
- Unauthorized changes to EFI partitions

Behavioral Indicators

- Systems unexpectedly booting into command shell environments before WinRE loads
- Unauthorized access to BitLocker-protected drives without normal authentication prompts
- Low-privileged accounts interacting with SYSTEM-trusted object paths
- Unexpected privilege escalation activity tied to CTFMON-related processes

Targeted Industries

Organizations using Microsoft Windows systems with BitLocker, Windows Recovery Environment (WinRE), or shared workstation/server environments may be impacted by these vulnerabilities.

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.

  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

GitHub - Nightmare-Eclipse/GreenPlasma: GreenPlasma Windows CTFMON Arbitrary Section Creation Elevation of Privileges Vulnerability · GitHub

Chaotic Eclipse: We're doing silent patches now huh, also a quick note about YellowKey