INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 10:49 UTC

RoguePlanet Zero-Day Exploits Microsoft Defender Race Condition for SYSTEM Privilege Escalation on Fully Patched Windows

SECURITY ANALYSIS | CRITICAL | CVSS 9.5

SCC Item ID	SCC-STY-2026-0193
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Microsoft Defender, Windows 10, Windows 11 (fully patched through June 2026 Patch Tuesday, including KB5094126 and KB5093998)
Published	2026-06-09T19:11:18
Discovery Source	Rss

Executive Summary

A publicly released exploit called RoguePlanet allows an attacker with local access to a Windows 10 or Windows 11 system to gain full administrative control, bypassing all security protections including Microsoft Defender, even on systems fully updated through the June 2026 Patch Tuesday cycle. As of the publication date, no fix from Microsoft has been issued, and the exploit code is actively circulating outside controlled repositories. Any organization running Windows endpoints should assume all managed and unmanaged Windows devices are at risk until Microsoft releases a patch.

Technical Analysis

RoguePlanet is a publicly available proof-of-concept exploit targeting a race condition (CWE-362) in Microsoft Defender on Windows 10 and Windows 11, including systems patched through the June 2026 Patch Tuesday cycle (KB5094126 and KB5093998). The vulnerability chain combines improper privilege management (CWE-269) and reference to an externally controlled resource (CWE-610) to spawn a SYSTEM-privileged command prompt from a standard user context. Exploitation maps to MITRE ATT&CK techniques T1068 (Exploitation for Privilege Escalation), T1574.010 (Services File Permissions Weakness), T1055 (Process Injection), and T1059.003 (Windows Command Shell). Third-party testing of this exploit has been reported by application control vendors. No CVE ID has been assigned. No vendor patch exists. The PoC is distributed on a self-hosted platform outside GitHub and GitLab controls. Source quality is T3 (BleepingComputer, ZDI, Thurrott); specific technical claims require corroboration from Microsoft Security Response Center or a CISA

advisory, neither of which has been issued at time of writing. CVSS scoring is pending official vendor evaluation; analyst assessment suggests a base score in the 9.0-9.5 range pending CVSS v3.1 assignment, but no official score is currently available.

Action Checklist

1. Step 1: Containment. Immediately audit all Windows 10 and Windows 11 endpoints for local user accounts and interactive session exposure. Restrict local logon rights to only authorized personnel via Group Policy (NIST AC-6, Least Privilege; CIS 5.4, Restrict Administrator Privileges to Dedicated Administrator Accounts). Disable or remove accounts that do not require local interactive access. For high-value systems, consider isolating from general network segments until a patch is available.
2. Step 2: Detection. Monitor for unexpected SYSTEM-level process spawning from Microsoft Defender service contexts. Query Windows Security event logs for Event ID 4688 (process creation) where the parent process is MsMpEng.exe or a Defender service and the spawned process is cmd.exe, powershell.exe, or similar. Enable and review NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) across all Windows endpoints. Alert on T1059.003 indicators: cmd.exe launching with SYSTEM token from non-standard parent. Cross-reference against CIS 8.2 (Collect Audit Logs) baseline to ensure endpoint logging is active.
3. Step 3: Eradication. No Microsoft patch is currently available. Apply compensating controls: enforce application allowlisting to restrict unauthorized process execution (NIST SI-4 equivalent behavioral monitoring). Evaluate application control solutions that restrict process execution by parent-child relationships and integrity level. Monitor Microsoft Security Response Center (https://msrc.microsoft.com) and CISA Known Exploited Vulnerabilities catalog for patch or advisory issuance. Do not rely on current Patch Tuesday updates (KB5094126, KB5093998) as remediation; verify independently via MSRC release notes whether they address this vulnerability chain.
4. Step 4: Recovery. Once Microsoft issues a patch, validate deployment across all Windows 10 and Windows 11 endpoints via patch management tooling. Confirm patch installation by verifying updated build numbers against Microsoft's bulletin. Post-patch, review SYSTEM-level process creation logs for any anomalous activity that may indicate prior compromise. Rotate credentials for any accounts that held local access during the exposure window (NIST AC-2, Account Management; D3-CRO, Credential Rotation).
5. Step 5: Post-Incident. Conduct a gap assessment against NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges) to identify any endpoints where standard users retain unnecessary local access. Review detection coverage for privilege escalation patterns (T1068) in your SIEM. Document this event as a case study for zero-day exposure in endpoint security tooling, notably that the security product itself was the attack surface. Validate that audit logging (CIS 8.2, NIST AU-2) is active and retained per policy (NIST AU-11, Audit Record Retention) on all endpoints.

Detection Guidance

Primary indicator: cmd.exe or powershell.exe spawned with a SYSTEM integrity token where the parent process is MsMpEng.exe, WinDefend service, or a Microsoft Defender-related binary. Query Windows Security Event ID 4688 (process creation with command line auditing enabled) for this pattern. Supplement with Sysmon Event ID 1 (process creation), filtering for ParentImage containing 'MsMpEng.exe' and IntegrityLevel of 'System'. Also monitor for unexpected scheduled task creation or service installation immediately following such process

spawning (T1574.010, T1055). IOC data (hashes, IPs, domains) is not available from public sources; behavioral detection based on process creation logs is the primary viable approach until the exploit is reverse-engineered or further disclosed. NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs) compliance is a prerequisite for this detection to function. Ensure command-line auditing is enabled in Windows Advanced Audit Policy: Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy > Detailed Tracking > Audit Process Creation.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOC URLs available`	PoC is circulating on a self-hosted platform outside GitHub and GitLab; no verified URL or hash has been published in available source reporting	LOW

Framework Mappings

MITRE-ATTACK

- **T1574.010** — Services File Permissions Weakness
- **T1210** — Exploitation of Remote Services
- **T1068** — Exploitation for Privilege Escalation
- **T1203** — Exploitation for Client Execution
- **T1055** — Process Injection
- **T1059.003** — Windows Command Shell

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-16** — Memory Protection
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1574.010	Services File Permissions Weakness	Persistence
T1210	Exploitation of Remote Services	Lateral-Movement
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1203	Exploitation for Client Execution	Execution
T1055	Process Injection	Defense-Evasion
T1059.003	Windows Command Shell	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-...	T3
Windows 11 KB5094126 & KB5093998 cumulative updates released	https://www.bleepingcomputer.com/news/microsoft/windows-11-kb509412.. .	T3
The June 2026 Security Update Review - Zero Day Initiative	https://www.zerodayinitiative.com/blog/2026/6/9/the-june-2026-secur...	T3
Microsoft Releases June 2026 Patch Tuesday Updates - Thurrott.com	https://www.thurrott.com/windows/337178/microsoft-releases-june-202...	T3

Source	URL	Tier
Windows 10 22H2 June 2026 Patch Tuesday security updates have ...	https://www.youtube.com/watch?v=2lJtS4VUFKc	T3

Generated 2026-06-12 10:49 UTC by TJS Security Command Center