INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-20 06:44 UTC

Sustained Windows Zero-Day Disclosure Cluster: YellowKey, GreenPlasma, MiniPlasma Demand Immediate Patch Prioritization

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0342
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Windows (specific versions not confirmed in available source data)
Published	2026-05-19T17:06:54
Discovery Source	Rss

Executive Summary

A security researcher has publicly disclosed three unpatched Windows zero-day vulnerabilities, YellowKey, GreenPlasma, and MiniPlasma, as part of a sustained disclosure campaign following Patch Tuesday. No CVE IDs have been assigned and Microsoft has not confirmed official patches, leaving Windows enterprise environments exposed to privilege escalation and memory corruption attack paths. The disclosure pace is outrunning Microsoft's patch cycle, multiplying unpatched exposure risk across potentially every Windows deployment in your organization.

Technical Analysis

Three Windows zero-days have been publicly disclosed by a security researcher under the names YellowKey, GreenPlasma, and MiniPlasma. Specific affected Windows versions are not confirmed in available source data, Microsoft MSRC should be treated as the authoritative source for version scope. No CVE IDs have been assigned. The vulnerability cluster spans four CWE classes: CWE-269 (improper privilege management), CWE-416 (use-after-free), CWE-787 (out-of-bounds write), and CWE-119 (improper restriction of memory buffer bounds). These map to MITRE ATT&CK techniques T1068 (exploitation for privilege escalation), T1203 (exploitation for client execution), T1211 (exploitation for defense evasion), and T1190 (exploit public-facing application). The mix of memory corruption classes (CWE-416, CWE-787, CWE-119) alongside privilege abuse (CWE-269) suggests potential chaining: memory corruption to gain code execution, privilege escalation to achieve persistence or lateral movement. No official patches exist as of the configuration date. No CVSS vector string, EPSS score, or KEV listing is available. CVSS base 7.5 (High) is sourced from secondary reporting (Dark

Reading) and is not official MSRC scoring; treat as unverified pending MSRC confirmation and CVE assignment. All specific technical details should be confirmed against Microsoft MSRC before operational decisions.

Action Checklist

1. Step 1: Containment. Monitor Microsoft MSRC (https://msrc.microsoft.com/update-guide/vulnerability) and the Microsoft Security Blog (https://www.microsoft.com/en-us/security/blog/threat-intelligence/vulnerabilities-and-exploits/) for any out-of-band advisories or emergency guidance related to YellowKey, GreenPlasma, or MiniPlasma. Until patches are available, assess which Windows systems are internet-facing or reachable by untrusted users and prioritize network segmentation or access restriction for those assets. Reduce attack surface by disabling unnecessary Windows components and services on exposed endpoints; test any component disablement in a non-production environment first to avoid unintended service disruption.
2. Step 2: Detection. Given that specific affected components are unconfirmed, focus detection on behavioral indicators consistent with the mapped MITRE techniques. For T1068 (privilege escalation): monitor Windows Security Event Log for Event ID 4672 (special privileges assigned to new logon) and Event ID 4673 (privileged service called) with unexpected source processes. For T1203 (client execution exploitation): monitor Sysmon Event ID 1 for unusual process spawning chains, particularly from Office, browser, or document-rendering processes. For T1190 (exploitation of public-facing application): review IIS and Windows application event logs for unexpected crashes or error spikes, which may indicate failed exploitation attempts (and precede successful ones). Enable and review Windows Defender Exploit Guard or Microsoft Defender for Endpoint alerts for memory corruption indicators. No confirmed IOCs are available for these vulnerabilities.
3. Step 3: Eradication. No official patches or mitigations have been released by Microsoft for YellowKey, GreenPlasma, or MiniPlasma as of the configuration date. Check Microsoft MSRC daily for patch availability. When patches are released, prioritize deployment to internet-facing Windows systems first, then internal servers, then endpoints. Apply patches within your organization's defined SLA for High-severity vulnerabilities. In the interim, apply available compensating controls: enable Windows Defender Exploit Guard memory protection features, enforce least privilege across service accounts, and restrict user-mode code execution where feasible.
4. Step 4: Recovery. After Microsoft releases and you deploy patches, validate remediation by confirming patch installation via your patch management platform (WSUS, SCCM, Intune, or equivalent) and cross-referencing against the applicable MSRC KB article numbers. Re-run vulnerability scans against previously exposed systems. Monitor for 72 hours post-patch for any anomalous privilege escalation or memory-related crash events that could indicate active exploitation attempts that preceded the patch.
5. Step 5: Post-Incident. This disclosure cluster exposes a structural gap: your patch prioritization process may not account for unpatched zero-days disclosed outside the standard Patch Tuesday cycle. Review and update your vulnerability management policy to include a defined response SLA for zero-days disclosed without an available patch. Confirm that your threat intelligence feeds provide timely coverage of researcher-disclosed vulnerabilities, not only CVE-assigned items. Assess whether Windows privilege escalation paths are adequately constrained by your current endpoint least-privilege posture.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/compliance if Event ID 4672 anomalies or WER crash dumps on systems containing PII, PHI, or PCI-scoped data are detected during the unpatched exposure window, or if any Windows system shows process lineage consistent with T1068/T1203 exploitation (document renderer or IIS worker process spawning cmd.exe, powershell.exe, or net.exe), as this may trigger breach notification obligations under HIPAA, PCI DSS, or applicable state privacy laws.
Recovery Notes	After MSRC patches for YellowKey, GreenPlasma, and MiniPlasma are deployed, verify installation using KB-specific 'Get-HotFix' queries on all previously internet-facing or untrusted-user-reachable Windows hosts and cross-reference against the MSRC advisory KB numbers. Monitor Windows Security Event Log (Event IDs 4672, 4673) and Sysmon Event ID 1 process creation chains for a minimum of 72 hours post-patch, as exploitation that occurred during the zero-day window may have established persistence via scheduled tasks, service installations, or registry run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) that will survive the patch. Any WER crash dumps or memory images collected from systems during the unpatched period should be preserved offline and analyzed for indicators of pre-patch exploitation before declaring full recovery.
Forensic Artifacts	Windows Error Reporting crash dumps at '%LOCALAPPDATA%\CrashDumps' and '%PROGRAMDATA%\Microsoft\Windows\WER\ReportQueue' — memory corruption exploits consistent with GreenPlasma and MiniPlasma will generate WER reports with stack traces pointing to the corrupted Windows component; these are the highest-value artifacts for confirming exploitation attempts before patch availability. | Windows Security Event Log Event ID 4672 (Special Privileges Assigned to New Logon) filtered on source processes other than known administrative binaries — YellowKey's privilege escalation path would manifest as an unexpected process receiving SeDebugPrivilege, SeImpersonatePrivilege, or SeTcbPrivilege outside of a standard logon sequence. | Sysmon Event ID 1 (Process Create) and Event ID 10 (ProcessAccess) logs showing cross-process memory access or unusual child process chains originating from IIS worker processes (w3wp.exe), Office application processes (WINWORD.EXE, EXCEL.EXE), or browser renderer processes — consistent with T1203 client-side exploitation and T1190 exploitation of public-facing applications mapped to this cluster. | IIS access logs at '%SystemDrive%\inetpub\logs\LogFiles\W3SVC*' showing HTTP 500 error spikes, unusual URI patterns, or repeated requests to the same endpoint from a single source IP — failed exploitation attempts against T1190-vulnerable Windows web components will appear as error bursts immediately preceding a successful exploitation event. | Windows registry persistence keys at 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run', 'HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks', and the Windows Services registry hive ('HKLM\SYSTEM\CurrentControlSet\Services') — post-exploitation persistence following a successful privilege escalation via YellowKey would most likely manifest as a new service installation or scheduled task created by the escalated process, visible in these keys with a creation timestamp during the zero-day exposure window.

Per-Action IR Details

Step 1: Containment — Monitor Microsoft MSRC (https://msrc.microsoft.com/update-guide/vulnerability) and the Microsoft Security Blog (https://www.microsoft.com/en-us/security/blog/threat-intelligence/vulnerabilities-and-exploits/) for any out-of-band advisories or emergency guidance related to YellowKey, GreenPlasma, or MiniPlasma. Until

patches are available, assess which Windows systems are internet-facing or reachable by untrusted users and prioritize network segmentation or access restriction for those assets. Reduce attack surface by disabling unnecessary Windows components and services on exposed endpoints.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For teams without enterprise NAC or SIEM: use Windows Firewall with Advanced Security (netsh advfirewall) to block inbound connections on affected endpoints — run 'netsh advfirewall set allprofiles firewallpolicy blockinbound,allowoutbound' on internet-facing hosts as an emergency posture. Enumerate internet-exposed Windows services using nmap ('nmap -sV -p 1-65535 ') to identify attack surface. Use osquery ('SELECT name, status FROM services WHERE status = "running"') to audit running services and disable non-essential ones via 'sc stop && sc config start=disabled'. Subscribe to MSRC RSS feed (https://msrc.microsoft.com/blog/feed) for out-of-band advisory alerts without requiring a SIEM integration.

Evidence: Before restricting access or modifying firewall rules, capture a point-in-time snapshot of the current network exposure: export Windows Firewall rule sets ('netsh advfirewall export C:\forensics\firewall_baseline.wfw'), enumerate all listening ports and associated processes ('netstat -ano > C:\forensics\netstat_baseline.txt'), and document running services via 'sc query type= all state= running > C:\forensics\services_baseline.txt'. This baseline is critical for distinguishing pre-containment exposure from post-containment anomalies, and establishes the attack surface that YellowKey, GreenPlasma, and MiniPlasma could have targeted before isolation.

Step 2: Detection — Given that specific affected components are unconfirmed, focus detection on behavioral indicators consistent with the mapped MITRE techniques. For T1068 (privilege escalation): monitor Windows Security Event Log for Event ID 4672 (special privileges assigned to new logon) and Event ID 4673 (privileged service called) with unexpected source processes. For T1203 (client execution exploitation): monitor Sysmon Event ID 1 for unusual process spawning chains, particularly from Office, browser, or document-rendering processes. For T1190 (exploitation of public-facing application): review IIS and Windows application event logs for unexpected crashes or error spikes, which may indicate failed exploitation attempts (and precede successful ones). Enable and review Windows Defender Exploit Guard or Microsoft Defender for Endpoint alerts for memory corruption indicators. No confirmed IOCs are available for these vulnerabilities.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR or SIEM, deploy Sysmon with a hardened configuration (SwiftOnSecurity or olafhartong/sysmon-modular config) to capture Event ID 1 (Process Create), Event ID 10 (ProcessAccess), and Event ID 8 (CreateRemoteThread) — the latter two are direct memory corruption and code injection indicators consistent with GreenPlasma and MiniPlasma's described attack paths. Write a PowerShell polling script to parse Security Event Log every 15 minutes for Event ID 4672 source processes outside of known admin accounts: 'Get-WinEvent -LogName Security -FilterXPath "*[System[EventID=4672]]" | Where-Object {$_.Properties[1].Value -notin $trustedAccounts}'. Deploy the public Sigma rule for T1068 (privilege escalation via exploit) converted to Windows Event Log XML queries using sigma-cli with the 'windows-audit' backend as a no-SIEM detection alternative.

Evidence: Capture Windows Security Event Log entries for Event IDs 4672 and 4673 filtering on non-standard source processes (i.e., privilege assignments originating from document renderers, browsers, or IIS worker processes — w3wp.exe, WINWORD.EXE, chrome.exe, msedge.exe). Export Sysmon Event ID 1 logs showing process lineage for any child processes spawned by these parent processes. For T1190-related exploitation of public-facing Windows services, extract IIS logs from '%SystemDrive%\inetpub\logs\LogFiles\W3SVC*' and Windows Application Event Log entries with Source 'W3SVC' or 'WAS' showing crash events (Event IDs 1000, 1001 in Application log). For memory corruption indicators consistent with MiniPlasma and GreenPlasma, collect Windows Error Reporting crash dumps

from '%LOCALAPPDATA%\CrashDumps' and '%PROGRAMDATA%\Microsoft\Windows\WER\ReportQueue', which may contain stack traces revealing the corrupted memory region.

Step 3: Eradication — No official patches or mitigations have been released by Microsoft for YellowKey, GreenPlasma, or MiniPlasma as of the configuration date. Check Microsoft MSRC daily for patch availability. When patches are released, prioritize deployment to internet-facing Windows systems first, then internal servers, then endpoints. Apply patches within your organization's defined SLA for High-severity vulnerabilities. In the interim, apply available compensating controls: enable Windows Defender Exploit Guard memory protection features, enforce least privilege across service accounts, and restrict user-mode code execution where feasible.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without enterprise patch management, use Windows Update for Business group policy or standalone 'wuauclt /detectnow /updatenow' to force update checks on individual hosts immediately upon MSRC patch release. Enable all available Windows Defender Exploit Guard protections via PowerShell: 'Set-ProcessMitigation -System -Enable DEP,SEHOP,ForceRelocateImages,BottomUp,HighEntropy' — these mitigations directly target the memory corruption exploitation path described for GreenPlasma and MiniPlasma. Enforce least privilege on service accounts using the built-in 'Local Security Policy' tool (secpol.msc) to audit and remove SeDebugPrivilege and SeImpersonatePrivilege from non-SYSTEM accounts, which are commonly abused in T1068 privilege escalation chains like YellowKey. Use 'icacls' to restrict write permissions on directories used by public-facing Windows services.

Evidence: Before applying any compensating controls or patches, document the current exploit mitigation posture of affected systems by running 'Get-ProcessMitigation -System' and saving output — this establishes a pre-remediation baseline to confirm that Exploit Guard configurations take effect. Export the current privilege rights assignments via 'secedit /export /cfg C:\forensics\secpol_baseline.cfg' to capture SeDebugPrivilege and SeImpersonatePrivilege holders before least-privilege enforcement. If any system shows evidence of prior exploitation (unexpected privilege assignments in Event ID 4672 logs, anomalous WER crash dumps), preserve a full memory image using WinPmem or Magnet RAM Capture before applying patches, as patching will overwrite exploit residue in memory and on-disk artifacts may be limited for fileless privilege escalation techniques.

Step 4: Recovery — After Microsoft releases and you deploy patches, validate remediation by confirming patch installation via your patch management platform (WSUS, SCCM, Intune, or equivalent) and cross-referencing against the applicable MSRC KB article numbers. Re-run vulnerability scans against previously exposed systems. Monitor for 72 hours post-patch for any anomalous privilege escalation or memory-related crash events that could indicate active exploitation attempts that preceded the patch.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without a patch management platform, validate KB installation on each Windows host using 'Get-HotFix -Id KB' or 'wmic qfe get HotFixID,InstalledOn | findstr KB' — substitute the MSRC-published KB number once available. For vulnerability re-scan without a commercial scanner, run Microsoft's free Safety Scanner (MSERT) or use OpenVAS/Greenbone Community Edition targeting previously exposed Windows hosts. For the 72-hour post-patch monitoring window, use a scheduled Sysmon log export script ('wevtutil qe Microsoft-Windows-Sysmon/Operational /f:text /rd:true /c:500 > C:\forensics\sysmon_postpatch_.txt') run every 6 hours, specifically hunting for Event ID 1 entries showing privilege escalation chains from the same parent processes (w3wp.exe, Office applications) that were flagged pre-patch.

Evidence: Post-patch, preserve evidence of the remediation action itself: export 'Get-HotFix' output listing installed KB numbers with timestamps ('Get-HotFix | Export-Csv C:\forensics\hotfix_log_postpatch.csv') to document the patch deployment timeline. Retain all pre-patch Sysmon logs, Security Event Logs (particularly Event IDs 4672, 4673, 4688), and WER crash dumps collected during the exposure window — these constitute the forensic record of the unpatched period and are required if a later investigation reveals exploitation occurred before patching. Continue collecting Windows Security Event Log Event ID 4688 (Process Creation) with command-line logging enabled to detect any post-exploitation persistence mechanisms (scheduled tasks, service installations, registry run keys) that may have been established during the zero-day exposure window.

Step 5: Post-Incident — This disclosure cluster exposes a structural gap: your patch prioritization process may not account for unpatched zero-days disclosed outside the standard Patch Tuesday cycle. Review and update your vulnerability management policy to include a defined response SLA for zero-days disclosed without an available patch. Confirm that your threat intelligence feeds provide timely coverage of researcher-disclosed vulnerabilities, not only CVE-assigned items. Assess whether Windows privilege escalation paths are adequately constrained by your current endpoint least-privilege posture.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a commercial threat intelligence platform, configure free monitoring of the following researcher-disclosure channels that surfaced YellowKey, GreenPlasma, and MiniPlasma: set up RSS monitoring of MSRC (https://msrc.microsoft.com/blog/feed), subscribe to the Full Disclosure mailing list (https://seclists.org/fulldisclosure/), and follow the relevant security researcher accounts on GitHub and social platforms where these disclosures originated. Use a shared spreadsheet or free Kanban tool (Trello, GitHub Projects) to track zero-day SLA timers for vulnerabilities without assigned CVEs, using disclosure date as the SLA start date. Conduct a tabletop exercise specifically simulating the YellowKey/GreenPlasma/MiniPlasma scenario — researcher discloses, no patch exists, disclosure is public — to validate your team's compensating control decision tree for this class of event.

Evidence: For the post-incident lessons-learned record, assemble the following documentation artifacts specific to this zero-day cluster exposure period: (1) the timeline of MSRC monitoring actions taken from disclosure to patch availability, (2) exported logs showing which Windows systems were internet-facing or reachable by untrusted users during the unpatched window (from the netstat and firewall baseline captures in Step 1), (3) any Event ID 4672/4673 anomalies detected during the exposure window, and (4) the WER crash dump inventory from exposed systems. This evidence package supports both the lessons-learned meeting and any regulatory notification assessment if PII or PHI systems were in the exposed asset set during the zero-day window.

Detection Guidance

No confirmed IOCs are available for YellowKey, GreenPlasma, or MiniPlasma. Detection must rely on behavioral indicators aligned to the mapped MITRE techniques. Focus on: (1) Privilege escalation signals, Windows Security Event IDs 4672, 4673, and 4674 from unexpected or low-privilege source processes; unexpected token impersonation via Event ID 4648. (2) Memory corruption exploitation precursors, application crashes or Windows Error Reporting (WER) entries for core Windows processes; Sysmon Event ID 1 for unusual parent-child process relationships involving system binaries. (3) Defense evasion (T1211), unexpected modifications to security tool processes or sudden gaps in endpoint telemetry. (4) Microsoft Defender for Endpoint: review alerts in the 'Suspicious process injection' and 'Potential privilege escalation' categories. Until MSRC confirms affected components, treat any unexplained privilege escalation or memory fault on Windows systems as potentially related. Specific log queries cannot be provided without confirmed affected component names, refine once MSRC publishes advisory details.

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1211** — Exploitation for Defense Evasion
- **T1068** — Exploitation for Privilege Escalation
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A03:2021** — Injection

CIS-V8

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

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
T1203	Exploitation for Client Execution	Execution
T1211	Exploitation for Defense Evasion	Defense-Evasion
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/windows-zero...	T3
Vulnerabilities - Security Update Guide - Microsoft	https://msrc.microsoft.com/update-guide/vulnerability	T1
Vulnerabilities and exploits | Latest Threats | Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/threat-intelligence/v...	T1
Security Update Severity Rating System - Microsoft	https://www.microsoft.com/en-us/msrc/security-update-severity-ratin...	T1
Microsoft Windows security vulnerability - BOXX Insurance USA	https://boxxinsurance.com/us/en/resources/microsoft-windows-securit...	T3

Generated 2026-05-20 06:44 UTC by TJS Security Command Center