Companion to: Critical Zero-Interaction Word/Outlook RCE

Reference Bulletin Date: May 14, 2026 | For internal use and client technical response | TLP: GREEN

Commands & Syntax Notice: Commands and code in this document are reproduced from cited sources as a reference only. Results may vary based on your environment, OS version, and tooling. Validate in a test environment before running in production.

IOC Notice: Indicators listed here reflect those reported by cited sources at the time of publication and are not exhaustive. Threat actor infrastructure evolves — consult current threat intelligence feeds and your EDR/SIEM for the most complete picture. Absence of these indicators does not confirm a clean environment.

1. PATCH VERIFICATION

1.1 Confirm Patch Deployment via Tenable

- Run Tenable Nessus Plugin **314343** against all Windows endpoints to identify hosts with unpatched Microsoft Word or Office installations: *(Source: Tenable)*
  - https://www.tenable.com/plugins/nessus/314343
  - Plugin covers: CVE-2026-40361, CVE-2026-40364, CVE-2026-40366, CVE-2026-40367, CVE-2026-40421, CVE-2026-35440 *(Source: Tenable)*
- Scope the scan to all endpoints with Microsoft Office installed — include workstations, jump hosts, and any RDS/Citrix session hosts.
- For environments using Tenable.io or Tenable.sc, filter findings by Plugin ID 314343 in the vulnerability dashboard to generate a remediation list.

1.2 Verify the Installed Office Build Manually

- Open any Office application → File → Account → About [Application]. The required minimum build to be protected: *(Source: Microsoft)*
  - Current Channel: Version 2604 (Build 19929.20164)
  - Monthly Enterprise Channel: Version 2604 (Build 19929.20162)
  - Monthly Enterprise Channel: Version 2603 (Build 19822.20240)
  - Monthly Enterprise Channel: Version 2602 (Build 19725.20320)
  - Semi-Annual Enterprise Channel: Version 2508 (Build 19127.20646)
  - Office 2024 Retail: Version 2604 (Build 19929.20164)
  - Office 2021 Retail: Version 2604 (Build 19929.20164)
  - Office LTSC 2024 Volume Licensed: Version 2408 (Build 17932.20776)
  - Office LTSC 2021 Volume Licensed: Version 2108 (Build 14334.20670)
  - Office 2019 Volume Licensed: Version 1808 (Build 10417.20132)

1.3 Confirm via Registry (Alternative)

- The Office build version is stored at: *(Source: Microsoft)*

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\ClickToRun\Configuration
```

  - Value: `VersionToReport` — compare against the minimum build numbers above.
- For MSI-based installs (Office 2019/2016): *(Source: Microsoft)*

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\16.0\Common\ProductVersion
```

2. COMPENSATING CONTROLS (PRE-PATCH)

2.1 Disable the Outlook Preview / Reading Pane

The Preview Pane is the primary zero-interaction attack vector for this vulnerability. Disabling it org-wide eliminates the attack surface for Outlook-delivered exploitation.

- **Outlook Desktop (per user):** *(Source: Microsoft)*

```
View → Reading Pane → Off
```

- **Group Policy (M365/Office 2019/2016 — ADMX):** *(Source: Microsoft)*
  - Path: `User Configuration → Administrative Templates → Microsoft Outlook 2016 → Outlook Options → Preferences → E-mail Options → Reading Pane`
  - Setting: `Do not use Reading Pane → Enabled`
- **Verify via GPO Result:** *(Source: Microsoft)*

```
gpresult /h gpresult.html /user <username>
```

2.2 Force Plain Text Email Reading

Prevents OLE and Word-rendering code paths from executing on email content. Note: this strips inline images and some formatting — communicate the change to users.

- **Outlook Desktop (per user):** *(Source: Microsoft)*

```
File → Options → Trust Center → Trust Center Settings → Email Security → ☑ Read all standard mail in plain text
```

- **Group Policy:** *(Source: Microsoft)*
  - Path: `User Configuration → Administrative Templates → Microsoft Outlook → Security → Automatic Picture Download`
  - Additionally set: `User Configuration → Microsoft Outlook → Outlook Options → Mail Format → Force plain text reading → Enabled`

2.3 Windows File Explorer Preview Pane

The same vulnerable Word parser is invoked when Office documents are previewed in Windows File Explorer. Disable the Explorer Preview Pane on high-risk hosts:

- **File Explorer:** View → Preview Pane → Toggle off *(Source: Microsoft)*
- **Group Policy:** *(Source: Microsoft)*
  - Path: `User Configuration → Administrative Templates → Windows Components → Windows Explorer`
  - Setting: `Turn off the display of snippets in Content view mode → Enabled`

3. DETECTION AND THREAT HUNTING

3.1 SentinelOne Deep Visibility — Anomalous Child Process

Hunt for unexpected processes spawning from OUTLOOK.EXE or WINWORD.EXE. Post-exploitation shellcode commonly spawns cmd.exe, PowerShell.exe, wscript.exe, or mshta.exe as children of Office processes.

- **Deep Visibility Query (S1 DV):** *(Source: Tenable, SC Media)*

```
EventType = "Process Creation" AND ParentProcessName ContainsCIS
"outlook.exe" OR "winword.exe" AND TgtProcName In ("cmd.exe",
"powershell.exe", "wscript.exe", "mshta.exe", "regsvr32.exe", "rundll32.exe",
"cscript.exe")
```

3.2 SentinelOne STAR Rule — Office Process Anomalous Children

Deploy this STAR rule to auto-alert on suspicious child process creation from Word or Outlook:

- **STAR Rule Logic:** *(Source: Tenable)*

```
EventType = "Process Creation" ParentProcessName ContainsCIS "outlook.exe" OR
"winword.exe" TgtProcName In ("cmd.exe", "powershell.exe", "wscript.exe",
"mshta.exe", "regsvr32.exe", "rundll32.exe", "cscript.exe") NOT
TgtProcCmdLine Contains "OfficeClickToRun"
```

    - Severity: High | Alert type: Threat | Auto-quarantine: Optional (validate before enabling)
- **Note:** Use OriginalFileName metadata as the primary match indicator — not process name alone — to prevent bypass via process renaming.

```
OriginalFileName In ("OUTLOOK.EXE", "WINWORD.EXE")
```

3.3 Anomalous Outbound Network from Office Processes

Monitor for network connections initiated by OUTLOOK.EXE or WINWORD.EXE to external, non-Microsoft IP ranges — a strong indicator of command-and-control (C2) callback post-exploitation:

- **Deep Visibility Query:** *(Source: Tenable, SC Media)*

```
EventType = "IP Connect" SrcProcName ContainsCIS "outlook.exe" OR
"winword.exe" NOT DstIP In (known-microsoft-ip-ranges) DstPort In (80, 443,
4444, 8080, 8443)
```

    - Baseline normal Microsoft 365 telemetry destinations first to reduce false positives — Microsoft CDN and update endpoints should be excluded.

3.4 Cisco FTD — Outbound from Workstation Subnets on Non-Standard Ports

- Alert on workstation-subnet IPs initiating outbound connections on ports not consistent with normal user traffic, particularly post-exploitation ports (4444, 1337, 8888): *(Source: SC Media)*

```
Access Policy → Add Rule: Source: <workstation-subnet> Destination: any-
external Port: 4444, 1337, 8888, 8080 (non-standard outbound) Action: Block +
Alert → Log to syslog
```

4. IOC REFERENCE

No confirmed threat-actor infrastructure IOCs (hashes, domains, IPs) are publicly available for CVE-2026-40361 as of the bulletin date. Active exploitation has not been confirmed in the wild. The indicators below are behavioral/process-based and should be monitored proactively.

Indicator	Type	Description	Source
`OUTLOOK.EXE spawning cmd.exe`	Behavioral	Post-exploitation process chain — unexpected child process from Outlook	Tenable / SC Media
`WINWORD.EXE spawning powershell.exe`	Behavioral	Post-exploitation process chain — unexpected child process from Word	Tenable / SC Media
`CWE-416 / Use-After-Free trigger`	Vulnerability Class	Memory corruption in Word parser (ole32 DLL code path)	Microsoft MSRC
`CVE-2026-40361`	CVE	Use-after-free in Microsoft Office Word — Preview Pane RCE	Microsoft MSRC
`CVE-2026-40364`	CVE	Type confusion in Microsoft Office Word — Preview Pane RCE (same patch)	Microsoft MSRC

When infrastructure IOCs become available, they will be published to ThreatFox (abuse.ch) and MSRC's updated advisory. Monitor: https://threatfox.abuse.ch and https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40361

5. MITRE ATT&CK MAPPING

Tactic	Technique	Notes
Initial Access	T1566.001 — Phishing: Spearphishing Attachment	Malicious document delivered via email; Preview Pane triggers exploit without attachment open
Execution	T1203 — Exploitation for Client Execution	CVE-2026-40361 exploited during document preview to execute arbitrary code
Persistence	T1547 — Boot/Logon Autostart (if post-exploit)	Attacker may drop persistence mechanism after initial code execution
Defense Evasion	T1055 — Process Injection (post-exploit)	Shellcode commonly injected into trusted processes after initial foothold
Command & Control	T1573 — Encrypted Channel	Post-exploit C2 callback over HTTPS to actor-controlled infrastructure