INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 07:27 UTC

CVE-2026-49494: Comodo Internet Security's firewall driver Inspect.sys contains an integer underflow in its IPv6 pac...

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0286
Type	CVE Vulnerability
CVE ID	CVE-2026-49494
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0007 (22th percentile)
Affected Products	Comodo Internet Security, firewall driver Inspect.sys (specific version range not specified in source data)
Published	2026-06-07T13:16:20.927
Discovery Source	Nvd

Executive Summary

A high-severity vulnerability in Comodo Internet Security's kernel-mode firewall driver (Inspect.sys) allows a remote, unauthenticated attacker to crash any protected Windows system by sending a single malformed IPv6 packet, with no open ports or user interaction required. The flaw exists in the driver's IPv6 packet parser, which runs before firewall rules are evaluated, making network-level controls ineffective as a defense. Organizations running Comodo Internet Security on Windows endpoints or servers face potential for targeted denial-of-service attacks against any internet-connected or network-reachable host.

Technical Analysis

CVE-2026-49494 is an integer underflow (CWE-191) in Comodo Internet Security's kernel-mode firewall driver Inspect.sys. The IPv6 packet parser decrements an unsigned 64-bit payload-length counter by the size of each IPv6 extension header without validating that the declared payload length is greater than or equal to the cumulative extension-header size. When a crafted packet declares a payload length smaller than the sum of its extension headers, the unsigned counter wraps to approximately 2^64. This triggers two downstream consequences on separate code paths: an out-of-bounds read (CWE-125) and an oversized memcpy (CWE-120), both executing at DISPATCH_LEVEL in the Windows kernel. Execution at DISPATCH_LEVEL means standard exception handling is unavailable, guaranteeing a BSOD (system crash). Exploitation requires

no authentication, no open ports, and no user interaction; a single crafted IPv6 packet is sufficient. The vulnerability maps to MITRE ATT&CK T1499.001 (Endpoint Denial of Service: OS Exhaustion Flood) and T1190 (Exploit Public-Facing Application). Affected product: Comodo Internet Security, specific version range not confirmed in available source data. Patch availability: not confirmed in source data. CVSS base score: 7.5 (High). EPSS: 0.0071% (21.8th percentile). Not currently listed on CISA KEV.

Action Checklist

1. Step 1: Containment. Identify all Windows endpoints and servers running Comodo Internet Security with Inspect.sys loaded. Until a patch is available and applied, consider temporarily disabling IPv6 on internet-facing interfaces where operationally feasible (Windows network adapter advanced settings or via Group Policy). This is a temporary measure only; re-enable IPv6 and restore normal configuration after Comodo releases and you apply the official patch. Consult the Comodo vendor advisory for official interim guidance before making changes. Note: disabling IPv6 may affect network functionality, validate in a test environment first.
2. Step 2: Detection. Query endpoint management tooling (EDR, SCCM, Intune) for presence of Inspect.sys across your asset inventory (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory; CIS 2.1, Establish and Maintain a Software Inventory). Review Windows Event Logs for unexpected BSOD events (Event ID 1001, BugcheckCode associated with kernel memory violations) on Comodo-protected hosts. Monitor network logs for anomalous IPv6 packets with malformed extension header chains from untrusted external sources (NIST AU-2, Event Logging; NIST AU-6, Audit Record Review, Analysis, and Reporting). No public IOCs (IPs, hashes, domains) are available for this CVE at time of writing.
3. Step 3: Eradication. Apply the official Comodo patch or updated Inspect.sys driver version as soon as Comodo releases it; monitor the official Comodo advisory channel for patch availability. Until patched, evaluate whether Comodo Internet Security can be temporarily replaced with an alternative endpoint protection solution on highest-risk hosts. If IPv6 is not operationally required on affected systems, disable it as a structural mitigation (NIST SI-4, System Monitoring; CIS 7.3, Perform Automated Operating System Patch Management; CIS 7.4, Perform Automated Application Patch Management).
4. Step 4: Recovery. After patching, verify Inspect.sys file version matches the vendor-confirmed patched version on all affected endpoints. Confirm no persistence of unexpected kernel crashes post-patch via Windows Reliability Monitor or endpoint management tooling. Re-enable IPv6 on interfaces where it was disabled as a temporary measure, after confirming the patched driver is in place. Resume normal monitoring posture and confirm endpoint protection is fully operational (NIST AU-6, Audit Record Review, Analysis, and Reporting; CIS 8.2, Collect Audit Logs).
5. Step 5: Post-Incident. Document any gaps in software inventory processes that delayed identification of Comodo-protected hosts (CIS 1.1, CIS 2.1). Evaluate the pre-firewall-rule execution behavior of all kernel-mode security drivers in your environment as a broader architectural review. Update vulnerability management process to include kernel-mode driver components of endpoint security products, which are often excluded from standard patch scanning (CIS 7.1, Establish and Maintain a Vulnerability Management Process; CIS 7.2, Establish and Maintain a Remediation Process). Consider D3-SFA (System File Analysis) controls to monitor Inspect.sys and similar kernel driver files for unauthorized modification.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and network operations if any Comodo-protected host shows Event ID 1001 BugcheckCode consistent with kernel pool corruption (0xc5, 0x19, 0x50) coinciding with inbound IPv6 extension header traffic, if internet-facing servers running Comodo are confirmed unpatched and IPv6 cannot be disabled within 4 hours, or if the organization operates in a regulated environment (HIPAA, PCI-DSS) where server availability loss constitutes a reportable incident.
Recovery Notes	After applying the vendor-released Inspect.sys patch, verify the updated driver file version and SHA-256 hash against Comodo's published patched values on every previously affected host before re-enabling IPv6 on those interfaces. Monitor Windows Application Event Log (Event ID 1001, BugcheckCode fields) and Sysmon Event ID 6 (DriverLoad) for 48 hours post-patch to confirm the patched driver handles IPv6 extension header chains without faulting. Retain the pre-patch vulnerable Inspect.sys hash, crash minidumps, and network captures as an evidence package for at minimum 90 days to support any post-incident review or regulatory inquiry.
Forensic Artifacts	C:\Windows\Minidump*.dmp and C:\Windows\MEMORY.DMP — kernel crash dumps generated when the integer underflow in Inspect.sys's IPv6 extension header parser triggers a BSoD; these will contain the faulting instruction pointer within Inspect.sys and the malformed packet data that triggered the fault | Windows Application Event Log Event ID 1001 (WER fault bucket) entries with BugcheckCode values indicating kernel memory violations (0xc5 DRIVER_CORRUPTED_EXPOOL, 0x19 BAD_POOL_HEADER, 0x50 PAGE_FAULT_IN_NONPAGED_AREA) on hosts with Inspect.sys loaded in kernel space | Network packet captures (PCAP) on internet-facing interfaces showing inbound IPv6 packets with anomalous extension header chaining (Next Header field values 0x00 hop-by-hop or 0x3C destination options with malformed length fields) delivered to Comodo-protected hosts immediately preceding any crash event | C:\Windows\System32\drivers\Inspect.sys — file metadata including version string, SHA-256 hash, digital signature timestamp, and last-modified date to confirm vulnerable version presence and establish pre-patch baseline | C:\ProgramData\Comodo\ directory logs — Comodo Internet Security application logs that may record driver fault events, firewall rule processing failures, or anomalous IPv6 packet events captured by the product before the crash occurs

Per-Action IR Details

Step 1: Containment — Identify all Windows endpoints and servers running Comodo Internet Security with Inspect.sys loaded. Until a patch is available and applied, consider temporarily disabling IPv6 on internet-facing interfaces where operationally feasible (Windows network adapter advanced settings or via Group Policy). Consult the Comodo vendor advisory for official interim guidance before making changes. Note: disabling IPv6 may affect network functionality — validate in a test environment first.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run the following PowerShell one-liner across all Windows hosts (via PSRemoting or manual execution) to identify systems with Inspect.sys loaded in kernel: `Get-WmiObject Win32_SystemDriver | Where-Object

{$_.PathName -like '*Inspect.sys*'} | Select-Object Name, State, PathName`. To disable IPv6 on all adapters without SCCM/GPO, execute: `Get-NetAdapterBinding -ComponentID ms_tcpip6 | Disable-NetAdapterBinding`. Document each host modified. For network-level pre-firewall blocking of malformed IPv6 extension headers, deploy a Wireshark/tshark capture filter on perimeter taps: `ip6 and ip6[6] != 59` to baseline extension header traffic before implementing upstream ACLs on edge routers.

Evidence: Before disabling IPv6, capture the current IPv6 interface configuration on each host (`Get-NetIPAddress -AddressFamily IPv6 | Export-Csv`) and the full Inspect.sys driver metadata including file version, hash (SHA-256 via `Get-FileHash C:\Windows\System32\drivers\Inspect.sys`), load status, and digital signature (`Get-AuthenticodeSignature`). Capture Windows System Event Log entries around any recent unexpected reboots that may indicate prior exploitation attempts triggering BSoD. Preserve upstream network flow/NetFlow data showing inbound IPv6 traffic to affected hosts for the prior 72 hours.

Step 2: Detection — Query endpoint management tooling (EDR, SCCM, Intune) for presence of Inspect.sys across your asset inventory (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory; CIS 2.1 — Establish and Maintain a Software Inventory). Review Windows Event Logs for unexpected BSOD events (Event ID 1001, BugcheckCode associated with kernel memory violations) on Comodo-protected hosts. Monitor network logs for anomalous IPv6 packets with malformed extension header chains from untrusted external sources (NIST AU-2 — Event Logging; NIST AU-6 — Audit Record Review, Analysis, and Reporting). No public IOCs (IPs, hashes, domains) are available for this CVE at time of writing.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR or SCCM, enumerate Inspect.sys presence using a PowerShell script deployed via scheduled task or manual run: `Get-ChildItem -Path C:\Windows\System32\drivers -Filter Inspect.sys -Recurse -ErrorAction SilentlyContinue | ForEach-Object { [PSCustomObject]@{ Host=$env:COMPUTERNAME; Path=$_.FullName; Version=(Get-Item $_.FullName).VersionInfo.FileVersion; Hash=(Get-FileHash $_.FullName -Algorithm SHA256).Hash } }`. For BSOD detection without SIEM, query Windows Application Event Log for Event ID 1001 (WER fault bucket, BugcheckCode) using: `Get-WinEvent -LogName Application | Where-Object {$_.Id -eq 1001 -and $_.Message -like '*BugCheck*'}`. For network-side detection, run a tshark capture on internet-facing interfaces to flag IPv6 packets with chained extension headers (hop-by-hop + destination options with anomalous length fields): `tshark -i eth0 -f 'ip6' -Y 'ipv6.nxt == 0 or ipv6.nxt == 60' -w inspect_ipv6_anomalies.pcap`. Write a Sigma rule targeting Event ID 1001 with BugcheckCode values associated with kernel pool corruption (0xc5, 0x19, 0x50) on hosts where Inspect.sys is confirmed loaded.

Evidence: Collect Windows Application Event Log Event ID 1001 entries (WER, BugcheckCode and BugcheckParameter fields) from all Comodo-protected hosts — the integer underflow in Inspect.sys during IPv6 extension header parsing would manifest as a kernel memory fault BSOD. Collect minidump files from `C:\Windows\Minidump\` and the full memory dump from `C:\Windows\MEMORY.DMP` on any host that crashed; these will contain the faulting instruction pointer within Inspect.sys's IPv6 parsing routine. Collect network captures or NetFlow records showing inbound IPv6 packets with malformed extension header length fields (Next Header chaining anomalies) delivered to affected hosts immediately preceding any crash events.

Step 3: Eradication — Apply the official Comodo patch or updated Inspect.sys driver version as soon as Comodo releases it; monitor the official Comodo advisory channel for patch availability. Until patched, evaluate whether Comodo Internet Security can be temporarily replaced with an alternative endpoint protection solution on highest-risk hosts. If IPv6 is not operationally required on affected systems, disable it as a structural mitigation (NIST SI-4 — System Monitoring; CIS 7.3 — Perform Automated Operating System Patch Management; CIS 7.4 — Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Without automated patch management, create a tracked remediation checklist per host using a CSV (hostname, Inspect.sys version, patch applied date, verified hash). For driver replacement: stop the Comodo Inspect.sys driver service before patch (`sc stop inspect`), apply the vendor-provided installer, then verify the updated driver is loaded (`sc query inspect`). If temporarily uninstalling Comodo on high-risk hosts, ensure Windows Defender is re-enabled immediately via PowerShell: `Set-MpPreference -DisableRealtimeMonitoring $false`. For IPv6 structural disable via Group Policy without SCCM, push a registry key: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters` — set `DisabledComponents` (DWORD) to `0xFF` (disables all IPv6 components) per Microsoft KB929852, and document each host where applied.

Evidence: Before patching, preserve a file system hash of the vulnerable Inspect.sys (`Get-FileHash C:\Windows\System32\drivers\Inspect.sys -Algorithm SHA256`) to establish a pre-patch baseline and confirm the vulnerable version is present. Capture the current driver signing certificate chain (`Get-AuthenticodeSignature C:\Windows\System32\drivers\Inspect.sys | Format-List`). If any host experienced a prior crash suspected to be CVE-2026-49494 exploitation, preserve the full contents of `C:\Windows\Minidump\` and `C:\ProgramData\Comodo\` logs before patching, as the patch process may overwrite relevant artifacts.

Step 4: Recovery — After patching, verify Inspect.sys file version matches the vendor-confirmed patched version on all affected endpoints. Confirm no persistence of unexpected kernel crashes post-patch via Windows Reliability Monitor or endpoint management tooling. Re-enable IPv6 on interfaces where it was disabled as a temporary measure, after confirming the patched driver is in place. Resume normal monitoring posture and confirm endpoint protection is fully operational (NIST AU-6 — Audit Record Review, Analysis, and Reporting; CIS 8.2 — Collect Audit Logs).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Verify patched Inspect.sys version and hash against the vendor advisory using: `(Get-Item C:\Windows\System32\drivers\Inspect.sys).VersionInfo.FileVersion` and `Get-FileHash C:\Windows\System32\drivers\Inspect.sys -Algorithm SHA256` — compare output against vendor-published patched version string and SHA-256. To confirm no residual crashes post-patch, query Windows Reliability Monitor data programmatically: `Get-WinEvent -LogName 'Application' | Where-Object { $_.Id -eq 1001 }` and filter for BugcheckCode entries on patched hosts over a 48-hour post-patch window. To re-enable IPv6 after confirming patch, reverse the registry key: set `DisabledComponents` back to `0x00` or remove it, and re-enable adapter binding: `Enable-NetAdapterBinding -Name '*' -ComponentID ms_tcpip6`.

Evidence: Post-patch, capture the new Inspect.sys file version and SHA-256 hash to confirm it matches vendor-published patched values — document this as your patch verification artifact. Run a 48-hour post-patch network capture on previously affected hosts using tshark filtering for IPv6 extension header anomalies to confirm the patched driver correctly handles malformed packets without crashing. Collect Windows System Event Log entries (Event ID 6005/6006 — system start/stop, and Event ID 41 — unexpected shutdown) to confirm no post-patch kernel panics occurred. Retain the pre-patch and post-patch hash comparison record as evidence of remediation for vulnerability management tracking.

Step 5: Post-Incident — Document any gaps in software inventory processes that delayed identification of Comodo-protected hosts (CIS 1.1, CIS 2.1). Evaluate the pre-firewall-rule execution behavior of all kernel-mode security drivers in your environment as a broader architectural review. Update vulnerability management process to include kernel-mode driver components of endpoint security products, which are often excluded from standard patch scanning (CIS 7.1 — Establish and Maintain a Vulnerability Management Process; CIS 7.2 — Establish and Maintain a Remediation Process). Consider D3-SFA (System File Analysis) controls to monitor Inspect.sys and similar kernel driver files for unauthorized modification.

NIST Phase: Post Incident

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AU-11 (Audit Record Retention)

Compensating: For ongoing kernel driver monitoring without a commercial file integrity tool, deploy a Sysmon configuration with EventType 'DriverLoad' (Sysmon Event ID 6) and add a YARA rule targeting Inspect.sys file path and known-vulnerable version string to flag any unexpected driver reloads or version downgrades. Schedule a weekly PowerShell script via Task Scheduler to enumerate all loaded kernel drivers and compare their SHA-256 hashes against a known-good baseline: `Get-WmiObject Win32_SystemDriver | Select-Object Name, PathName | ForEach-Object { Get-FileHash $_.PathName -Algorithm SHA256 -ErrorAction SilentlyContinue }`. For inventory gap closure, add `Inspect.sys` and the parent Comodo Internet Security product explicitly to your vulnerability scanner's software detection profile, as kernel-mode drivers are frequently missed by agent-based scanners that enumerate only installed MSI/EXE packages.

Evidence: Retain all minidump files from `C:\Windows\Minidump\`, pre- and post-patch Inspect.sys file hashes, the remediation tracking CSV, and network captures of anomalous IPv6 extension header traffic per NIST AU-11 (Audit Record Retention) for the organization's defined retention period. Document the timeline from CVE-2026-49494 disclosure to full inventory identification and patch deployment — this gap metric directly feeds the vulnerability management process improvement required by CIS 7.2. Archive the Sysmon Event ID 6 (DriverLoad) baseline for Inspect.sys across all hosts as the authoritative known-good driver fingerprint for future integrity comparisons.

Detection Guidance

No public IOCs are available for CVE-2026-49494 at this time. Detection focuses on host-side crash telemetry and network anomaly patterns. On Windows hosts running Comodo Internet Security: query for Windows Error Reporting events (Event ID 1001 in the Application log, source 'Windows Error Reporting', BugcheckCode values associated with kernel memory access violations such as 0x50 PAGE_FAULT_IN_NONPAGED_AREA or 0xC5 DRIVER_CORRUPTED_EXPOOL). Correlate BSOD events with the presence of Inspect.sys in the crash dump's loaded module list. On the network side: inspect IPv6 traffic for packets with extension header chains where the declared payload length field (bytes 4-5 of the IPv6 fixed header) is smaller than the cumulative size of the extension headers present. This malformed structure violates RFC 8200 and should never appear in legitimate traffic, making it a high-confidence detection signal with minimal false positive risk. IDS/IPS signatures targeting malformed IPv6 extension header sequences may provide early warning. No vendor-confirmed detection rules or Sigma/Snort rules are publicly available for this CVE as of the configuration date. Applies NIST AU-2, AU-6, AU-12 and CIS 8.2.

Framework Mappings

MITRE-ATTACK

- **T1499.001** — OS Exhaustion Flood
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-16** — Memory Protection
- **AT-2** — Literacy Training and Awareness

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

OWASP-TOP10-2021

- **A03:2021** — Injection

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1499.001	OS Exhaustion Flood	Impact
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-49494	T1
CVE-2026-49494 - Vulnerability Details	https://app.opencve.io/cve/CVE-2026-49494	T3
CVE-2026-49494: Integer Underflow (Wrap or Wraparound) in ...	https://radar.offseq.com/threat/cve-2026-49494-integer-underflow-wr...	T3
CVE-2026-49494	https://vuldb.com/cve/CVE-2026-49494	T3
IPv6 Packet Parser Vulnerability in Kernel-Level Driver	https://threat-modeling.com/comodo-firewall-driver-integer-underflo...	T3

Generated 2026-06-10 07:27 UTC by TJS Security Command Center