



VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2026-03

CVE ID: CVE-2026-62748

Severity: High

CVSS v3.1 Score, 7.0 (High)

(CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

First Published: September 30, 2026

Last Update: September 30, 2026

Status: Confirmed

Revision: 1.0

Executive Summary

A race condition vulnerability (CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization) has been identified in the Microsoft Windows Telephony Service (TapiSrv). An authenticated attacker with existing low-privilege local execution access on the host operating system can exploit this vulnerability to achieve Local Privilege Escalation (LPE) to SYSTEM privileges.

This vulnerability stems from the underlying Windows operating system environment and impacts Windows-based VIVOTEK Network Video Recorders (NVR) and Video Management Software (VMS) host servers. This vulnerability cannot be exploited remotely on its own.

Overview:

Vulnerability Type	Local Privilege Escalation (LPE) / Race Condition
Common Weakness Enumeration	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization
Attack Vector	Local (AV:L)
Attack Complexity	High (AC:H) - Timing/race window condition dependent
Privileges Required	Low (PR:L) - Requires authenticated local account on the Windows host
User Interaction	None (UI:N)
Impact Scope	Confidentiality: High Integrity: High Availability: High

Affected Products:

Product Line / Model	Operating Environment / Platform	Vulnerability Status
VIVOTEK Windows-based NVR (e.g., NR Series) & PC Servers	Windows 10, Windows 11, Windows Server 2016 / 2019 / 2022 / 2025	AFFECTED (Prior to Aug 2026 Patch)
VAST Security Station (VSS) / VAST 2 Management Software	Running on supported Microsoft Windows platforms	AFFECTED (Host OS dependency)

Unaffected Products (Confirmed Safe):

- All VIVOTEK Standalone Embedded Linux NVRs
- All VIVOTEK IP Network Cameras and Edge AI Sensors
- VIVOTEK Cloud / VSaaS Core Services

Workaround:

1. Disable Windows Telephony Service (TapiSrv).

VIVOTEK NVR and VMS application suites (VAST / VSS) do not require the Windows Telephony Service. Disabling TapiSrv closes the attack vector completely with zero impact on surveillance, live viewing, or recording functions.

Execute in an Administrative PowerShell Terminal:

```
Stop-Service -Name "TapiSrv" -Force  
Set-Service -Name "TapiSrv" -StartupType Disabled
```

Verify service status:

```
Get-Service -Name "TapiSrv" | Select-Object Name, Status, StartType
```

2. Principle of Least Privilege & Account Hardening.

Enforce strict host access control: Restrict interactive logon, PowerShell remoting, and Remote Desktop (RDP) rights to designated domain/local administrators only.

Ensure surveillance operators and security guard personnel only interact with the VMS client application interface and possess no underlying OS logon credentials.

Isolate NVR host management interfaces on a dedicated Management VLAN with ingress firewall filtering.

Solution:

- 1. The primary and permanent resolution is to apply official Microsoft Security Updates released in August 2026 or subsequent cumulative rollups addressing CVE-2026-62748.**
- 2. Standard Remediation Procedure:**
 - a. Navigate to Windows Settings > Update & Security > Windows Update.
 - b. Click Check for updates and download/install all applicable Cumulative Updates released from August 2026 onwards.
 - c. Reboot the host system to finalize installation of the patched binaries.
 - d. For air-gapped / isolated surveillance networks: Obtain the standalone MSU package corresponding to your OS build from the Microsoft Update Catalog and deploy via internal patch management tools

Revision History:

Revision	Date	Description
1.0	October 1, 2026	First published