

Schwachstellen bei der Validierung ungültiger Eingaben in NI-PAL

Aktualisiert am 9. Juni 2026

Überblick

In NI-PAL wurden kürzlich zwei Sicherheitslücken bei der Validierung ungültiger Eingaben entdeckt. Diese Sicherheitslücken betreffen NI-PAL 26.3.0 und ältere Versionen unter Windows, Linux und Linux Real-Time.

[CVE-2026-8035](#) ermöglicht es einem lokal authentifizierten Benutzer möglicherweise, einen Denial-of-Service-Angriff auszulösen, indem er aufgrund einer NULL-Pointer-Dereferenzierung einen Absturz verursacht.

[CVE-2026-8036](#) ermöglicht es einem lokal authentifizierten Benutzer möglicherweise, auf beliebigen Systemspeicher zuzugreifen, was unter Umständen zu einer Rechteausweitung führt.

Viele NI-Treiber enthalten NI-PAL und sind von diesen Sicherheitslücken betroffen. Im Abschnitt „Abhilfemaßnahmen“ finden Sie Informationen zur Ermittlung der installierten NI-PAL-Version sowie Anleitungen zum Aktualisieren oder Installieren des Patches.

Inhalt

- [Leitfaden zur Schadensbegrenzung](#)
- [Betroffene Produkte](#)
- [CVSS-Score](#)
- [NI-Aktualisierungsdienst](#)
- [Weitere Informationen](#)
- [Danksagungen](#)
- [Zusätzliche Ressourcen](#)

Leitfaden zur Schadensbegrenzung

NI empfiehlt dringend, die betroffene Software zu aktualisieren, um diese Sicherheitslücken zu beheben. Informationen zur Aktualisierung dieser Produkte finden Sie im Abschnitt „Betroffene Produkte“.

NI-PAL ist eine gängige Komponente vieler NI-Treiber. Sie müssen nur einen NI-Treiber aktualisieren, der diese Komponente enthält, oder den Patch einmal pro Rechner installieren. Der Patch ist abwärtskompatibel mit früheren Versionen der NI-Software.

Diese Sicherheitslücke betrifft NI-PAL 26.3.0 und ältere Versionen. Um die installierte NI-PAL-Version zu ermitteln, folgen Sie den Anweisungen für Ihr Betriebssystem.

Wie kann NI Nigel AI Ihnen heute helfen?

Windows

Installierte NI-PAL-Version ermitteln

1. Navigieren Sie zum Ordner `%WinDir%\system32\drivers`.
2. Suchen Sie die Datei `nipalk.sys`. Klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie **Eigenschaften**.
3. Navigieren Sie im **Eigenschaftenfenster** zur Registerkarte „**Details**“. Notieren Sie sich die im Feld „**Produktversion**“ angegebene Version.
4. Falls die NI-PAL-Version 26.3.0 oder älter ist, installieren Sie den Patch für Windows.

Linux-Desktop

Installierte NI-PAL-Version ermitteln

- Verwenden Sie den Paketmanager Ihrer Distribution, um die Version des ni-pal-Pakets anzuzeigen.

ODER
- Führen Sie den folgenden Befehl aus, um die Version des geladenen NI-PAL-Kernelmoduls anzuzeigen:
`dkms status | grep nipalk`

Falls die NI-PAL-Version 26.3.0 oder älter ist, aktualisieren Sie die NI-Treiberversion.

Upgrade für Linux

1. Installieren Sie [die NI Linux-Gerätetreiber 2026 Q2](#) gemäß den [Standardanweisungen](#).
2. Installieren Sie die neuesten Updates über die Terminaleingabeaufforderung.

- Ubuntu
 - `sudo apt-get update && sudo apt-get upgrade`
- Red Hat Enterprise Linux
 - `sudo dnf upgrade`
- openSUSE Leap
 - `sudo zypper refresh && sudo zypper update`

NI Linux Echtzeit

1. Installieren Sie das [NI Linux RT System Image 2026 Q2](#) auf dem Host.
2. [Wenden Sie das Linux RT-Systemabbild 2026 Q2](#) auf das Zielsystem an.
3. Installieren Sie die neuesten Updates. Geben Sie dazu an der Eingabeaufforderung eines Host-Terminals Folgendes ein:

- `ssh <Benutzername>@<Zielhostname oder -adresse>`
- Geben Sie gegebenenfalls die Anmeldeinformationen des Zielsystems ein.
- An der Eingabeaufforderung der SSH-Sitzung:
 - `sudo opkg update && sudo opkg upgrade 'ni-pal'`

Wie kann NI Nigel AI Ihnen heute helfen?

Betroffene Produkte

Produktversion	Minderung
NI-PAL 26.3.0 und frühere Versionen	Windows: Installieren Sie NI-VISA 2026 Q2 Patch 1 (26.3.1) oder eine spätere Version über den NI Package Manager oder die Software-Downloads oder installieren Sie den Patch über den NI Update Service. Linux-Desktop: Installieren Sie die NI Linux-Gerätetreiber ab Version 2026 Q2. Hinweise zur Risikominderung finden Sie hier. NI Linux Real-Time: Installieren Sie das NI Linux RT System Image 2026 Q2 oder höher. Hinweise zur Risikominderung finden Sie hier.

CVSS-Score

- CVE-2026-8035 – 7.1 – CVSS:3.1 [AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H](#)
- CVE-2026-8035 – 6.9 – CVSS:4.0 [AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N](#)
- CVE-2026-8036 – 7.1 – CVSS:3.1 [AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N](#)
- CVE-2026-8036 – 8.4 – CVSS:4.0 [AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N](#)

NI-Aktualisierungsdienst

Der NI-Update-Dienst ist ein Windows-Dienstprogramm, das nach Aktualisierungen für NI-Software und -Treiber sucht und diese bereitstellt, einschließlich Sicherheitsupdates. Er kann manuell nach Aktualisierungen suchen, so konfiguriert werden, dass er regelmäßig nach Aktualisierungen sucht und Benutzer benachrichtigt oder Aktualisierungen automatisch zu einem festgelegten Zeitpunkt herunterlädt und installiert.

Einige der in dieser Empfehlung beschriebenen Maßnahmen empfiehlt ein Upgrade auf [NI Update Service 2026 Q1](#) oder Update Service kann separat installiert werden und ist abwärtskompatibel mit älterer NI-Software.

Wie kann NI Nigel AI Ihnen heute helfen?

Weitere Informationen

Bei NI betrachten wir die Sicherheit unserer Produkte als wichtigen Bestandteil unseres Engagements gegenüber unseren Kunden. Besuchen Sie ni.com/security, um sich über Sicherheitswarnungen und -probleme zu informieren und entsprechend zu handeln.

Danksagungen

NI möchte Patrick Saif (@weezerOSINT) für die Meldung dieses Problems und die Zusammenarbeit bei der koordinierten Offenlegung danken.

Zusätzliche Ressourcen

- [CVE-2026-8035](#) – Nationale Schwachstellendatenbank
- [CWE-476](#) – Dereferenzierung eines Nullzeigers
- [CVE-2026-8036](#) – Nationale Schwachstellendatenbank
- [CWE-1285](#) – Fehlerhafte Validierung des angegebenen Index, der Position oder des Offsets in der Eingabe

Wie kann NI Nigel AI Ihnen heute helfen?