Kritisches Sicherheitsupdate

Wenn Sie NI-Treibersoftware Version **Q2 2026 oder früher** verwenden, besuchen Sie ni.com/ni-pal-update und folgen Sie zum Schutz Ihrer Systeme den empfohlenen Schritten.

Erforderliches NI-PAL-Sicherheitsupdate

Aktualisiert am 8. Oktober 2026

Überblick

Zum Schutz unserer Systeme empfehlen wir allen Kunden, die NI-PAL-Versionen vor dem dritten Quartal 2026 verwenden, ein Sicherheitsupdate zu installieren. NI-PAL, eine in vielen NI-Treibern verwendete Komponente, steht aufgrund der in CVE-2026-18485 beschriebenen Sicherheitslücken auf der Microsoft-Sperrliste für anfällige Treiber . Ab dem 10. November 2026 kann Windows das Laden betroffener NI-PAL-Komponenten blockieren, sobald die Sperrliste aktiviert ist. Wird das Update nicht installiert, funktionieren NI-Software- und Hardware-Workflows nach einem Windows-Sicherheitsupdate möglicherweise nicht mehr.

Dieses gezielte Update betrifft nur eine Komponente. Es erfordert kein Treiber-Upgrade und ist abwärtskompatibel mit früheren NI-PAL-Versionen bis mindestens NI-PAL 17.0.

Inhalt

- Auswirkungen der NI-PAL-Sperre auf die Kunden
- Wer sollte Maßnahmen ergreifen?
- Erforderliche Maßnahmen – NI-PAL-Version prüfen und aktualisieren
- Zusätzliche Hinweise
- Zusätzliche Ressourcen

Auswirkungen der NI-PAL-Sperre auf die Kunden

Bereits ab dem 10. November 2026 werden Systeme, die nicht aktualisiert wurden, auf verschiedene Fehler im NI Measurement & Automation Explorer (MAX), im NI Hardware Manager oder in Gerätetreibern stoßen.

Wer sollte Maßnahmen ergreifen?

Kunden, die NI-Software oder -Hardware unter Microsoft Windows verwenden, sollten die installierte NI-PAL-Version überprüfen. Systeme mit NI-PAL 26.3.1 oder älter sind betroffen und sollten aktualisiert werden. Die Sperrliste für anfällige Treiber ist unter Windows 11 standardmäßig aktiviert, unter Windows 10 jedoch nicht. Die Einstellungen können jedoch vom Kunden oder der IT-Abteilung geändert worden sein.

Spezielle Anweisungen für Kunden des NI Semiconductor Test Systems (STS)

NI STS-Kunden sollten die Schritte im Dokument „NI-PAL 2026 Q3 Security Update: Options for STS Customers“ befolgen .

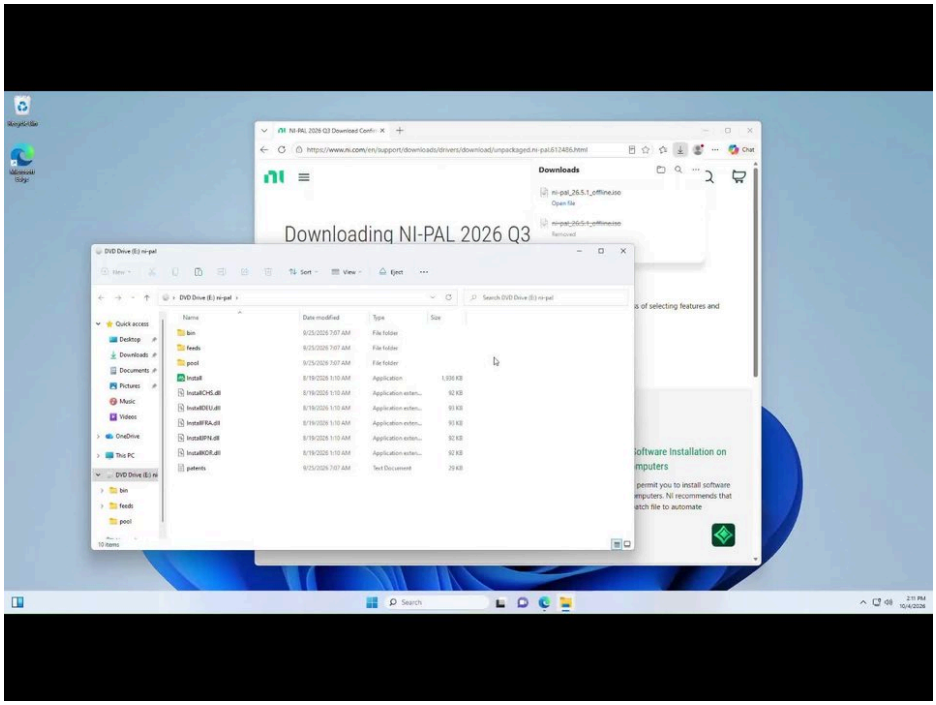
Spezielle Hinweise für NI SystemLink™ Softwarekunden

Anweisungen zur Verwendung von NI SystemLink zum Aktualisieren mehrerer betroffener Systeme finden Sie unter „ Aktualisieren betroffener Systeme auf NI-PAL 2026 Q3 mit NI SystemLink“.

Erforderliche Maßnahmen – NI-PAL-Version prüfen und aktualisieren

1. **Überprüfen Sie die installierte Version –** Öffnen Sie %WinDir%\system32\drivers, suchen Sie nipalk.sys, öffnen Sie Eigenschaften und überprüfen Sie die Produktversion auf der Registerkarte Details.
2. **Installieren Sie das Update –** Falls Ihre Version 26.3.1 oder älter ist, installieren Sie NI-PAL 2026 Q3 oder höher mithilfe des NI Update Service oder des Offline-Installers von der NI-PAL-Downloadseite .
   Hinweis : Wenn Sie den NI Update Service verwenden, müssen Sie möglicherweise zuerst den NI Package Manager aktualisieren, um das verfügbare Update anzuzeigen.
3. **Starten Sie das System neu –** Die Installation des Updates dauert etwa eine Minute und erfordert einen Neustart.
4. **Funktionsprüfung –** Nach dem Neustart führen Sie die unten empfohlenen Validierungsprüfungen durch.
   - Prüfen Sie, ob das Gerät in NI MAX oder NI Hardware Manager verfügbar ist.
   - Führen Sie einen Geräte-Selbsttest und einen Reset durch.
   - Führen Sie ein Testpanel oder ein Beispielprogramm aus, das die Hardware nutzt.

Das folgende Video zeigt den kompletten Upgrade-Prozess.



Zusätzliche Hinweise

- Wir raten davon ab, die Microsoft-Sperrliste für anfällige Treiber als allgemeine Problemumgehung zu deaktivieren. Dies kann den Schutz von Windows vor bekannten anfälligen Kernel-Treibern verringern.
- Zum Zeitpunkt der Veröffentlichung der Quelle waren keine Exploits für CVE-2026-18485 bekannt.
- Die Windows-Sperrliste wird nur auf Windows-Systemen durchgesetzt. Wir empfehlen Linux-Kunden, zusätzlich die aktuellen Sicherheitshinweise zu beachten, um rechtzeitig über kritische und sicherheitsrelevante NI-Software-Updates informiert zu werden und ihre Software bei Bedarf zu aktualisieren, um die Sicherheit zu gewährleisten.
- Kunden sollten die Benachrichtigungen des NI Update Service aktivieren und die NI-Sicherheitshinweise abonnieren, um über zukünftige Updates informiert zu werden.

Zusätzliche Ressourcen

- Lesen Sie die Sicherheitswarnung zu CVE-2026-18485.
- Erhalten Sie Informationen zu NI-Sicherheitswarnungen und zum Abonnement.
- Aktivieren Sie die regelmäßige Überprüfung im NI-Update-Dienst.

Sollten Sie Fragen oder Bedenken haben oder dieses Thema weiter besprechen wollen, zögern Sie bitte nicht, sich an unser technisches Support-Team zu wenden .

Windows ist eine Marke der Microsoft-Unternehmensgruppe.

Die eingetragene Marke Linux® wird gemäß einer Unterlizenz von LMI, dem exklusiven Lizenznehmer von Linus Torvalds, dem weltweiten Inhaber der Marke, verwendet.