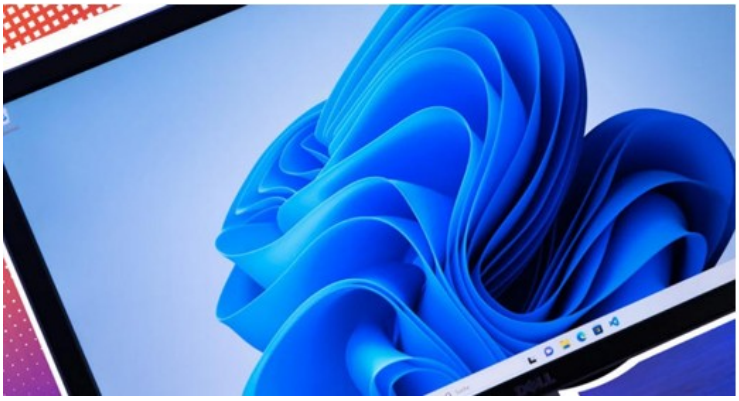
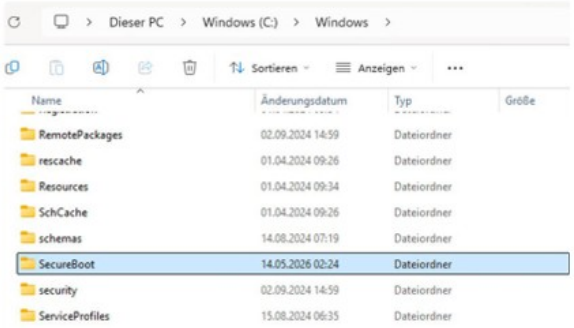
Mysteriöser Ordner in Windows 11 aufgetaucht.Darum solltet ihr ihn nicht löschen

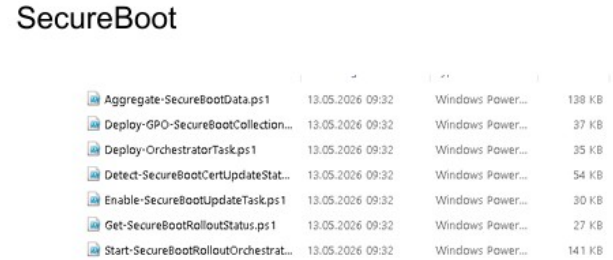


Nach der Installation des Windows-11-Updates KB5089549 haben viele Nutzer eine unerwartete Entdeckung gemacht. Im Windows-Systemverzeichnis ist ein neuer Ordner mit dem Namen „SecureBoot“ aufgetaucht. Microsoft hatte den „Überraschungs-Ordner“ in Windows 11 zunächst nicht in den Update Informationen erwähnt, sodass unklar war, ob Nutzer ihn löschen dürfen. Inzwischen hat das Unternehmen aber offiziell seine Existenz bestätigt und den Zweck von SecureBoot erklärt.

Was macht der Überraschungs-Ordner in Windows 11?

Der Hintergrund ist eine notwendige Sicherheitsmaßnahme. Die Zertifikate für den sicheren Systemstart (Secure Boot), die seit 2011 im Einsatz sind, verlieren im Juni 2026 ihre Gültigkeit. Ohne rechtzeitige Aktualisierung verlieren Windows-Systeme schrittweise den Schutz gegen Bootkit-Malware. Bei Windows 10 Rechnern, die mit dem Programm Rufus trotz Installationssperre manipuliert wurden, ist auf diesen Schutz wissentlich verzichtet worden. Sie sind damit gegen diese Rootkits, manipulierte Bootloader oder Schadcode auf Firmware beim Start weiterhin nicht geschützt. Um bei den übrigen Rechnern die System sicherheit durchgehend zu gewährleisten, verteilt Microsoft deshalb schrittweise die neuen „Secure Boot 2023“-Zertifikate über die monatlichen Windows-Updates. Der neue Ordner ist Teil dieses Prozesses. Obwohl der Ordner auf allen Windows11-Systemen erscheint, ist sein Inhalt vor allem für IT-Administratoren in Unternehmen relevant. Er enthält mehrere Skripte, mit denen Profis die Aktualisierung der neuen Zertifikate in großen Netzwerken verwalten können (Quelle: Microsoft)





SecureBoot-Ordner löschen oder nicht?

Sie müssen also nichts unternehmen, sollten den Ordner aber auch nicht manuell löschen. Die Experten von Windows Latest empfehlen hier, den Secure-Boot-Ordner einfach unangetastet zu lassen, da er nichts auf eurem PC tatsächlich verändert. Möglicherweise wird

er aber noch für ein zukünftiges Update benötigt. Falls nicht, wird ihn Microsoft voraussichtlich selbst wieder entfernen (Quelle: Windows Latest). Wer den Status der eigenen Zertifikate der originalen Windows 11 Hardware prüfen möchte, kann dies in der App „Windows-Sicherheit“ unter dem Punkt „Gerätesicherheit“ bei „Sicherer Start“ tun. Ein grüner Haken signalisiert hier, dass alles ordnungsgemäß funktioniert. Ist dort dagegen ein gelber oder roter Marker, solltet ihr aktiv werden. Wichtige, alte Windows-Zertifikate laufen ab: Neue Warnfunktion verwirrt Nutzer

Microsoft hat bekannt gegeben, dass wichtige Sicherheitszertifikate für Secure Boot im Juni 2026 auslaufen werden. Dies kann zu Sicherheitsproblemen führen, wenn keine Up dates der Zertifikate durchgeführt werden. Windows-Nutzer sollten sicherstellen, dass sie die neuesten Zertifikate installieren, um die Sicherheit und Wartungsfreundlichkeit ihrer Systeme zu gewährleisten

PC Welt informiert

Das passiert mit Ihrem Windows ab Juni, wenn Sie die Secure-Boot-Deadline übersehen

Was passiert mit Ihrem Windows-Rechner, wenn er in den nächsten Tagen nicht die neuen Secure-Boot-Zertifikate bekommt? Plus: So prüfen Sie, ob Ihr PC die neuen Zertifikate bereits besitzt.

Microsoft hat endlich konkret verraten, was mit Ihrem Windows-Rechner passiert, wenn dessen Secure-Boot-Zertifikate nicht vor Juni 2026 erneuert werden.

Im Juni 2026 laufen die originalen Secure-Boot-Zertifikate ab, mit denen Windows seit 2011 jede Hardware signierte. “Secure Boot ist ein von Vertretern der PC-Branche entwickelter Sicherheitsstandard, der sicherstellt, dass ein Gerät ausschließlich mit Software startet, der der Originalhersteller (OEM) vertraut“, fasst es Windowslatest zusammen. Bei jedem PC-Start überprüft die Firmware die kryptografische Signatur jeder einzelnen Boot-Softwarekomponente. Dazu gehören auch die Secure-Boot-Zertifikate, die 2011 ausgegeben wurden. Erst danach wird der Windows-Boot-Manager geladen.

Mit dem Ablauf der vorhandenen Secure-Boot-Zertifikate würden **Millionen Windows-PCs ab Juni unsicher werden oder überhaupt nicht mehr booten** (siehe hierzu Ihr Windows-PC bekommt ab Sommer echte Probleme – der Grund). Um das zu verhindern, liefert Microsoft seit einiger Zeit neue Secure-Boot-Zertifikate an die Rechner aus beziehungsweise trifft dafür Vorbereitungen.

Die Auslieferung dieser neuen “**2023er Secure Boot”-Zertifikate** ist keine triviale Angelegenheit, weil diese direkt in die UEFI-Hardware der Hauptplatine Ihres Rechners eingreifen. “Microsoft muss die neuen Zertifikate aus dem Jahr 2023 in die Firmware übertragen, den Boot-Manager durch eine mit den neuen Schlüsseln signierte Version ersetzen und schließlich das Vertrauen in die alten Zertifikate aufheben”, beschreibt Windowslatest den komplexen Vorgang.

Microsoft hat dafür bereits einen neuen Secure-Boot-Ordner auf den Windows-Rechnern eingerichtet, wie wir in Mysteriöser ‘**Secure Boot’-Ordner in Windows 11** aufgetaucht: Das steckt dahinter berichtet haben. In diesem Ordner speichert Windows die kryptografischen Dateien, bevor sie auf Ihr Motherboard übertragen werden.

Das sind die Folgen, wenn Sie die neuen Secure-Boot-Zertifikate nicht installieren

Um über die Folgen der ganzen Angelegenheit zu informieren, hat Microsoft eine “Fragestunde” mit Principal Security Engineer Arden White, Principal Software Architect Scott

Shell und Group Engineering Manager Richard Powell dazu veranstaltet. Die US-amerikanische IT-Nachrichtenseite Windowslatest nahm daran teil und fasst die Ergebnisse zusammen. Demnach lassen sich die Folgen für Windows-PCs mit veralteten, abgelaufenen Secure-Boot-Zertifikaten folgendermaßen zusammenfassen:

Wenn Sie die Frist für das Secure-Boot-Zertifikat im Juni 2026 ignorieren, starten Ihre Windows-11-PCs zwar weiterhin und laufen normal, doch die Systemsicherheit wird dauerhaft beeinträchtigt, da Microsoft keine bootkritischen Updates und Malware-Blacklists (DBX-Sperrlisten) mehr bereitstellt. Sie können den Secure-Boot-Status in der Windows-Sicherheits-App überprüfen.

Wenn Sie das neue Secure-Boot-Zertifikat für 2023 nicht installiert haben, wird Ihr PC den neuesten Windows Boot Manager nicht ausführen. **Daher wird Microsoft Ihnen keine Sicherheitsupdates mehr für bootkritische Binärdateien zur Verfügung stellen**. Außerdem kann Ihr System keine neuen DBX-Sperrlisten mehr herunterladen, wodurch Sie dauerhaft der **Gefahr durch zukünftige Bootkit-Malware ausgesetzt** sind. Zudem werden sich künftige Windows-Updates, die neue Funktionen für das Betriebssystem bringen, nicht mehr installieren lassen.

Sehr alte Rechner, die noch nicht UEFI, sondern BIOS nutzen, sollen von dem Problem nicht betroffen sein und das entsprechende Update auch nicht bekommen. Microsoft ergänzt, dass es vollkommen normal sei, dass Ihr Windows-Rechner für die Installation der neuen Secure-Boot-Zertifikate mehrmals neu startet. Eine eventuell vorhandene Bitlocker-Verschlüsselung muss nicht aufgehoben werden. In komplexen Unternehmensumgebungen können aber zusätzliche Maßnahmen erforderlich sein.

Die neuen 2023er-Secure-Boot-Zertifikate gelten bis 2038.

In den Windows-Einstellungen können Sie unter “Datenschutz und Sicherheit, Windows-Sicherheit, Gerätesicherheit” prüfen, ob mit Secure Boot auf Ihrem Rechner alles in Ordnung ist. Erscheint dort bei “Sicherer Start” ein kleiner grüner Kreis mit einem weißen Haken darin, dann passt alles: Alle neuen Secure-Boot-Zertifikate sind installiert und Ihr Windows-Rechner ist somit fit für die Juni-2026-Deadline.

Erscheint dort dagegen ein gelber oder roter Alarm, dann sollten Sie die dort angebotenen weiterführenden Informationen lesen.