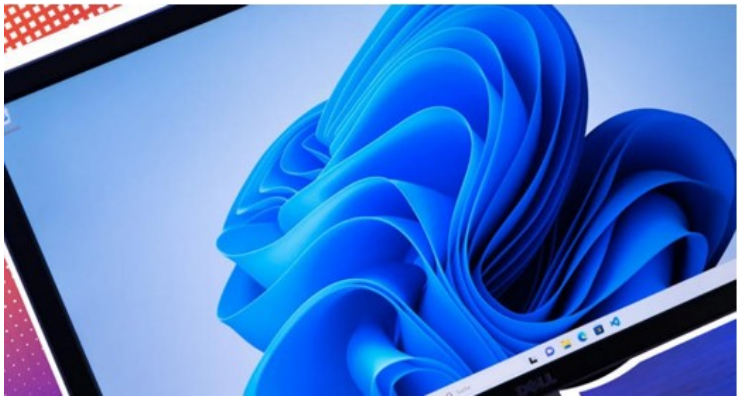
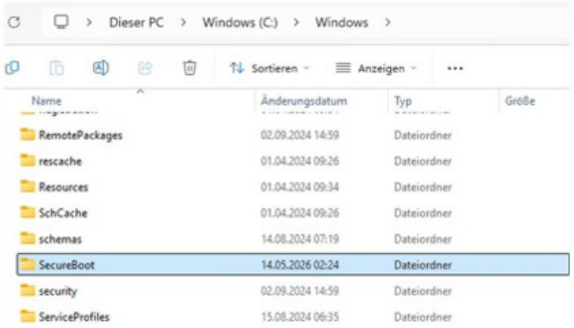
Mysteriöser Ordner in Windows 11 aufgetaucht.Darum solltet ihr ihn nicht löschen

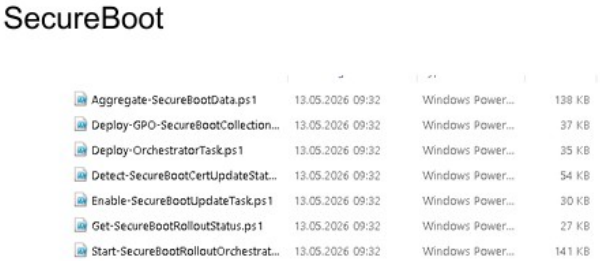


Nach der Installation des Windows-11-Updates KB5089549 haben viele Nutzer eine unerwartete Entdeckung gemacht. Im Windows-Systemverzeichnis ist ein neuer Ordner mit dem Namen „SecureBoot“ aufgetaucht. Microsoft hatte den „Überraschungs-Ordner“ in Windows 11 zunächst nicht in den Update Informationen 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.

Microsoft gibt (vorerst) Entwarnung für Secure Boot Deadline im Juni

Microsoft erklärt, warum der **24. Juni als Stichtag** für die neuen Secure Boot Zertifikate nicht so ausschlaggebend ist wie gedacht. Dennoch sollten bestimmte Anwender vorsichtig sein, wenn sie Secure Boot nicht rechtzeitig aktualisieren.In den letzten Monaten hatten wir über eine wichtige Umstellung von Zertifikaten in Windows 11 berichtet, die für den sicheren Systemstart benötigt werden. Microsoft informierte immer wieder darüber, dass Windows-PCs ab Juni ernste Probleme bekommen, sollten die nötigen Zertifikate nicht rechtzeitig aktualisiert werden.

Nun hat Microsoft gegenüber Windowslatest einige offene Fragen zum Thema Secure Boot beantwortet und gibt in einigen Punkten Entwarnung. **Der 24. Juni ist demnach nicht als “harte” Deadline zu sehen, nach deren Ablauf es für betroffene Systeme gar nicht mehr möglich sein wird, den sicheren Systemstart zu nutzen.**

Stattdessen soll sich diese Deadline speziell auf die Auslieferung eines Key Exchange Keys beziehen, der als **Sicherheitsschlüssel für Secure Boo**t dient. Daneben gibt es noch einen zweiten Schlüssel, den DB Key, der erst im Oktober 2026 ablaufen soll. **Wenn Sie bis zum 24. Juni nicht alle neuen Secure-Boot-Zertifikate bekommen haben, ist also noch nicht alles verloren**. Microsoft erwartet, mithilfe des zweiten Schlüssels noch bis Oktober weitere Boot Manager ausliefern zu können.

„Es gibt kein Ablaufdatum, ab dem der Registrierungsschlüssel und das Update nicht mehr funktionieren“, bestätigte Scott Shell, der als Principal Software Design Engineer bei Microsoft arbeitet.
Dennoch gibt es gewisse Einschränkungen, die nach Juni für alle Systeme gelten, die Secure Boot nicht aktualisiert haben. **Ihr System kann etwa keine neuen DBX-Sperrlisten mehr herunterladen** (diese enthalten die Signaturen fehlerhafter oder gefährlicher Bootloader, die Ihrem System schaden können, und daher von Windows blockiert werden).

Was ist, wenn ich Secure Boot nicht nutze?

Microsoft hat noch eine weitere, wichtige Frage beantwortet: Was passiert mit all den Systemen, die Secure Boot aktuell nicht aktiviert haben, es in Zukunft aber eventuell nutzen möchten?

Wenn Secure Boot deaktiviert ist, kann Microsoft die nötigen Zertifikate nicht aktualisieren. Das ist kein Problem, wenn es dabei bleibt (auch wenn der sichere Systemstart empfehlenswert ist, um Ihren PC vor Gefahren zu schützen.)

Shell erklärte, dass Microsoft auf diesen Rechnern dennoch den Boot-Manager auf die für 2023 signierte Version aktualisieren wird. Der Boot-Manager selbst ist also einsatzbereit, dennoch werden **aber die passenden Zertifikate benötigt.** Sind diese nicht vorhanden, kann es passieren, dass der Rechner gar nicht mehr startet.

Vor der ersten Aktivierung von Secure Boot muss also jeder Nutzer oder System-Admin dafür sorgen, dass zuerst die aktuellen Zertifikate manuell heruntergeladen werden. Das genaue Vorgehen hierfür hat Microsoft in diesem Support-Dokument festgehalten.

Gibt es Unterschiede zwischen Windows 11 und Windows 10?

Auf die Frage, ob es Unterschiede zwischen den Secure-Boot-Updates von Windows 10 und Windows 11 gibt, antwortete Microsoft mit **Nein**. Windows 10 bekommt im Rahmen der erweiterten Sicherheitsupdates noch bis Oktober relevante Sicherheitspatches, und die Secure Boot Zertifikate gehören hier dazu.
Der einzige Unterschied ist, dass einige **ältere Systeme nicht standardmäßig mit aktiviertem Secure Boot ausgeliefert wurden oder mit Konfigurationen laufen, die keine Telemetriedaten an Microsoft senden.** In diesem Fall müssen Sie etwas nachhelfen, um die Zertifikate zu erhalten.
Prüfen Sie am besten mithilfe dieser Anzeige, ob Secure Boot aktiviert wurde, und laden Sie die Zertifikate dann manuell herunter. Microsoft betont: Je früher die Zertifikate aktualisiert werden, desto besser.

Windows 10 bekommt ein weiteres Jahr lang Updates

Sensation: Microsoft verlängert den Supportzeitraum für Windows 10 um ein weiteres Jahr. Bis zum 12.10.2027 bleibt Windows 10 damit sicher. Das müssen Sie jetzt wissen.
Das ist aber sehr eigenartig:
Microsoft hat erst neulich u.a. darauf aufmerksam gemacht:
„Was macht der Überraschungs-Ordner in Windows 11? Der Hintergrund ist eine notwendige Sicherheitsmaßnahme. **Die Zertifikate für den sicheren Systemstart**

(Secure Boot, tpm), die seit 2011 im Einsatz sind, verlieren im Juni 2026 ihre Gültigkeit. Ohne rechtzeitige Aktualisierung auf Windows 11 verlieren Windows-Systeme schrittweise den Schutz gegen Bootkit-Malware.
D.h. im Klartext: alle Windows 10 Rechner sind gegen Bootkits nicht mehr geschützt, da die Zertifikate ja abgelaufen sind

Eigentlich sollten die Windows 10 Extended Security Updates (**ESU**) am 12. Oktober 2026 enden. Doch Microsoft beugt sich der Realität und den nach wie vor hohen Nutzerzahlen von Windows 10 und verlängert den Supportzeitraum um ein weiteres Jahr.

Microsoft nimmt diese Verlängerung völlig überraschend und ohne viel Tamtam vor und stellt die Änderung in diesem Blogbeitrag vor. Die Konsequenzen für Windows-10-Nutzer sind aber gravierend: **Sie können ihr Betriebssystem jetzt bis zum 12. Oktober 2027 sicher verwenden**. Denn bis zu diesem Datum stellt Microsoft kostenlose Sicherheits-Updates für Windows 10 bereit. Einzige Voraussetzung ist die Anmeldung zum ESU-Programm.

Sie finden diese wichtige Änderungen auch hier im offiziellen Microsoft-Dokument zu den Windows 10 Consumer Extended Security Updates (ESU) (hier die deutsche Fassung). Dort steht dieser folgenschwere Satz:

Der Support für Windows 10 ist ausgelaufen. Sie können sich jederzeit bis zum Ende des Programms am 12. Oktober 2027 für ESU anmelden. Wenn Sie bereits angemeldet sind, läuft Ihr Support automatisch bis zu diesem Datum weiter – Sie müssen nichts unternehmen.

Die Updates gibt es für Windows 10 Version 22H2 Home, Professional, Pro Education oder Workstations Edition. Dieses ESU-Programm gibt es zudem nur für Privatanwender-Rechner und nicht für den Einsatz von Windows 10 im Unternehmenseinsatz. Für Windows 10 im Unternehmenseinsatz gibt es ein eigenes, allerdings kostenpflichtiges ESU-Programm.

Einen offiziellen Grund für die überraschende Verlängerung nennt Microsoft nicht. Doch der Grund dürfte in den nach wie vor hohen Nutzerzahlen zu suchen sein: **Windows 11 verliert in Deutschland Marktanteile** – das ist der überraschende Gewinner.
Ohne Teilnahme am kostenlosen ESU-Programm endete der Support für Windows 10 bereits am 14. Oktober 2025.

Alles, was Sie zum ESU-Programm für Windows 10 wissen müssen, lesen Sie in **Windows 10 gratis sicher nutzen**: So registrieren Sie sich jetzt für das Windows 10 ESU-Programm.


Ihr Windows-PC ist in Gefahr.docx

Ihr Windows-PC ist in Gefahr, wenn Ihnen diese Sicherheitszertifikate fehlen: So lösen Sie das Problem

Das Thema Secure Boot ist noch nicht abgeschlossen. Microsoft stellt derzeit ein Update für eine größere Anzahl betroffener Computer bereit, doch möglicherweise benötigt Ihr PC Hilfe, um dieses Update zu erhalten.

Sie haben in letzter Zeit wahrscheinlich unzählige Warnmeldungen zu Windows und ablaufenden Secure-Boot-Zertifikaten gesehen.

Warum? **Einige PCs haben die Updates noch nicht erhalten (obwohl Microsoft noch ein Notfall-Update veröffentlicht hat) – und werden sie auch nicht erhalten, solange Sie nicht selbst Maßnahmen ergreifen.**

Das ist das erste Problem. Das zweite? Auch wenn Sie Ihren Rechner entsprechend vorbereiten, erhalten Sie die neuen Zertifikate möglicherweise nicht sofort.

Hier erfahren Sie, was Sie wissen sollten, damit Sie online sicher bleiben, bis Ihr PC die erforderlichen Updates erhält. Und wie Sie feststellen können, ob Ihr PC dieses Update überhaupt erhalten wird.

Tipp: Für eine tiefgreifende Analyse zum Thema Secure Boot und den möglichen Folgen eines fehlenden Updates empfehlen wir diesen Artikel: **Ihr Windows-PC bekommt ab Juni ernste Probleme – das können Sie (PC Welt)**

Was ist Secure Boot?

Beim Hochfahren lädt Ihr PC den erforderlichen Code, um Windows zu starten. Früher war diese Startsequenz nicht geschützt, also nutzten Hacker diese Lücke, um Malware zu entwickeln, die genau hier ansetzen und sich zudem der Erkennung durch Antivirensoftware entziehen konnte.

Microsoft hat Secure Boot (“sicherer Systemstart”) eingeführt, um solche Angriffe zu blockieren. Stellen Sie sich das ähnlich wie an einem Kontrollpunkt vor, an dem ein Beamter Ihren Ausweis überprüft, nachsieht, ob die Angaben mit denen in seiner Datenbank übereinstimmen, und Sie nur durchlässt, wenn Sie auf der Genehmigungsliste stehen.

Auf Ihrem PC entsprechen die Sicherheitszertifikate von Secure Boot dieser „Datenbank“. Um beim Systemstart ausgeführt zu werden, muss die „Identität“ (digitale Signatur) von Treibern, Software usw. mit den in den Zertifikaten gespeicherten Informationen übereinstimmen.

Einige PCs verwenden noch immer ältere Secure-Boot-Zertifikate, die im Jahr 2011 ausgestellt wurden. **Drei der vier Zertifikate sind in der letzten vollen Woche im Juni 2026 abgelaufen.** Das letzte läuft im Oktober 2026 ab. Für einen umfassenden Schutz sollte Ihr Computer neuere Secure-Boot-Zertifikate verwenden, die im Jahr 2023 ausgestellt wurden.

So erkennen Sie, ob Sie abgelaufene Secure-Boot-Zertifikate haben

Secure Boot warning - June 2026

Eine Warnung bezüglich eines Secure-Boot-Zertifikats in der Windows-Sicherheits-App.

Sie können einen PC auch ohne aktuelle Secure-Boot-Zertifikate weiterhin betreiben. Gehen Sie also nicht davon aus, dass alles in Ordnung ist, nur weil Ihr PC noch hochfährt.

Viele PCs haben jedoch bereits automatische Upgrades auf die Secure-Boot-Zertifikate von 2023 erhalten. Falls dies bei Ihrem PC nicht der Fall ist, sollte Windows Sie auf das Problem hinweisen – achten Sie auf ein **blaues Schildsymbol in der Taskleiste,** das entweder mit einer gelben oder einer roten Markierung versehen ist.

Sie sehen keine solche Warnung? Überprüfen Sie dies noch einmal, indem Sie die neue Secure Boot Anzeige öffnen. Suchen Sie nach Windows Sicherheit, wählen Sie dort Gerätesicherheit und schauen Sie auf das Symbol neben dem Begriff Secure Boot. Ein grünes Häkchen bedeutet, dass alles in Ordnung ist. Eine gelbe oder rote Warnanzeige bedeutet, dass Sie Maßnahmen ergreifen müssen.

Drei Maßnahmen, die Sie ergreifen sollten, wenn Ihre Secure-Boot-Zertifikate abgelaufen sind

Wenn Sie eine gelbe oder rote Warnung bezüglich Secure Boot sehen, müssen Sie Ihren PC überprüfen, um festzustellen, ob er diese automatischen Updates empfangen kann. Microsoft weitet die Einführung automatischer Zertifikatsupdates aus, kann diese neueren Zertifikate jedoch nicht bereitstellen, wenn Ihre Firmware veraltet ist.

Sobald Sie diese Frage geklärt haben, müssen Sie außerdem einige Vorsichtsmaßnahmen ergreifen, während Sie auf die aktualisierten Secure-Boot-Zertifikate warten.

Benötigt mein Windows 10 PC ebenfalls das neue Secure-Boot-Update?
Wenn Ihr Hersteller eine UEFI-Firmware mit einer relativ hohen Versionsnummer (z. B. über 8000) anbietet, enthält sie häufig Unterstützung für moderne Sicherheitsfunktionen. Ob **Secure Boot** und **TPM 2.0** tatsächlich vorhanden und aktivierbar sind, **hängt jedoch vom Mainboard und der Hardware ab.**

Warum startet mein Windows 11 PC während der Zertifikats-Aktualisierung mehrfach neu?
Welche Windows 11 Versionen erhalten das wichtige Sicherheits-Update automatisch?
Benötige ich für die neuen Zertifikate ein BIOS-Update meines Mainboard-Herstellers?
Was passiert mit meinem PC, wenn ich die erste Zertifikats-Deadline verpasse?