Dateibenachrichtigungssysteme machen Windows, Linux, Android und macOS angreifbar

28.9.2026 - | Technische Universität Graz

Ein Forschungsteam der TU Graz zeigt, wie über File Notifications verschiedener Betriebssysteme die Aktivitäten von Nutzer*innen ausgespäht und Passwortfenster gefälscht werden können.

Forschende am Institute of Information Security der TU Graz haben Sicherheitsrisiken in den Dateibenachrichtigungssystemen (File Notification Systems) der weit verbreiteten Betriebssysteme Windows, Linux, Android und macOS entdeckt. Durch sogenannte Seitenkanalangriffe ist es möglich, systemweit Änderungen an Dateien, Tastaturanschläge und besuchte Websites mitzuverfolgen sowie Passwortabfragefenster zu fälschen und so Passworteingaben abzufangen. Ihre Erkenntnisse haben die Forschenden in dem Paper "File Notification Attacks: Templating and Exploiting Side-Channel Leakage from the File-Notification Systems on Linux, Windows, and macOS" zusammengefasst und auf der eigens eingerichteten Website https://inoti.fyi publiziert.

Umweg über lesbare Ordner

Dateibenachrichtigungssysteme überwachen in Betriebssystemen, ob Dateien erstellt, gelöscht, geöffnet, geschlossen oder geändert werden und liefern dazu automatisch Systembenachrichtigungen, damit Anwendungen oder das System auf die Änderung reagieren können. Das Forschungsteam hat entdeckt, dass Apps oder andere Nutzer*innen auf demselben System auch ohne Administrator-Rechte diese Benachrichtigungen mitverfolgen können. Dadurch lässt sich nachvollziehen, was andere Nutzer*innen auf dem System tun. Notwendig dafür sind nur Leserechte auf bestimmte Ordner, wobei dadurch alle in einem Ordner abgelegten Dateien sowie die Unterordner und die dort enthaltenen Inhalte auslesbar werden, auch wenn diese eigentlich keinen Lesezugriff erlauben. Für alle Systeme gilt dabei, dass Dateiinhalte nicht auslesbar sind, sondern nur Dateinamen und ob Veränderungen stattgefunden haben. Das genügt aber, um das Verhalten der Nutzer*innen, des Systems und von Anwendungen mitzuverfolgen.

Browserverlauf nachvollziehbar

Wie solche Angriffe aussehen könnten, zeigt das Forschungsteam anhand von Fallbeispielen. Um bei Windows die Sperre des Lesezugriffs auf Ordner und Dateien zu umgehen, brauchten die Forschenden nur das Dateibenachrichtigungssystem des nicht lesegeschützten übergeordneten Verzeichnisses anzuzapfen. Mithilfe der Benachrichtigungen für das Hauptverzeichnis C:\ entdeckte das Team, dass sich alle Dateisystem-Ereignisse in allen Unterordnern mitverfolgen ließen – die Dateinamen eingeschlossen. Da Browser wie Firefox für jede besuchte Website, die den lokalen Speicher benötigt, einen eigenen Ordner anlegen, der den Namen der Website enthält, können Angreifende recht einfach und in Echtzeit nachvollziehen, wo sich die Nutzer*innen im Internet aufgehalten haben.

Abfangen von Tastenanschlägen und Passwörtern

Auf Linux nutzten die Forschenden das Dateibenachrichtigungssystem „inotify“, um innerhalb einer eigentlich lesegeschützten Datei die Tastenanschläge mitzuverfolgen. Linux unterband dabei zwar zunächst das direkte Überwachen der Datei, da sie aber in einem lesbaren Ordner lag, ließ sich dieser über das Benachrichtigungssystem ausspähen und machte dadurch die Tastenanschläge in der lesegeschützten Datei sichtbar. Welche Tasten betätigt worden sind, konnte das Team zwar nicht sehen, aber diese sogenannten Inter-Keystroke Timing Attacks gibt es bereits seit mehr als zwei Jahrzehnten. Durch das in diesen Jahren angesammelte wissen verrät mittlerweile alleine die Zeit, die zwischen den einzelnen Tastenanschlägen vergeht, einige Informationen.

Auf KDE Plasma, einer beliebten Desktop-Umgebung von Linux, gelang es den Sicherheitsforschenden, gefälschte Passworteingabefenster über die echten zu legen, sobald eine Authentifizierungsabfrage aufgerufen wurde. Das gelang auch, wenn das sichere Wayland Display-Server-Protokoll im Einsatz war, das die Kommunikation zwischen Anzeige und den darauf laufenden Programmen regelt. Dafür überwachten sie die Ausführungsdatei der Programmierschnittstelle „polkit“, die Autorisierungsprüfungen durchführt. Sobald ein Zugriff erkannt wurde, der ein Passwortfenster öffnet, legten die Testangreifenden ein gefälschtes Passwortfenster darüber, damit die Nutzer*innen dort ihre Eingaben tätigen und ihre Passwörter preisgeben.

Datenaustausch über WhatsApp

Unter Android soll das System „FUSE“ eigentlich verhindern, dass Apps Zugriff auf die Ordner anderer Apps haben. Nicht einmal der Inhalt dürfte erkennbar sein. Über den Umweg der Dateibenachrichtigungen gelang es aber trotzdem, dass eine App ohne besondere Rechte die Vorgänge in einem fremden Ordner ausspionieren konnte. So konnte das Team beobachten, ob Bilder, Videos und Dateien in den Ordnern von WhatsApp ankamen, gesendet oder gelöscht wurden. Die Forschenden betonen, dass sie keine Einsicht in die Dateiinhalte hatten, aber sie konnten die Dateinamen auslesen, die gegebenenfalls etwas über den Dateiinhalt und das Verhalten der Nutzer*innen des Android-Telefons verraten.

Obwohl macOS über die systemweit auslesbaren Files am wenigsten preisgab, fand das Team heraus, dass das Verhalten von Nutzer*innen, Anwendungen und des Systems dennoch mitverfolgt werden kann. So liefert die macOS-Programmierschnittstelle (API) „FSEvents“ verwertbare Einblicke in die Aktivitäten der User*innen.

Wie in solchen Fällen üblich, hat das Forschungsteam die Teams von Linux, KDE, Android, Microsoft und Apple bereits frühzeitig auf die möglichen Einfallstore hingewiesen, damit sie vor Veröffentlichung des Papers darauf reagieren können. Gemeinsam mit dem Linux-Sicherheitsteam wurden auch bereits Patches ausgerollt, die einige der Lücken entfernt haben.

Publikation: File Notification Attacks: Templating and Exploiting Side- Channel Leakage from the File-Notification Systems on Linux, Windows, and macOS
Autor*innen: Sudheendra Raghav Neela, Xufan Zhao, Jeanette Angelika Wultsch, Hannes Weissteiner, Florian Draschbacher, Stefan Gast, Daniel Gruss
Abrufbar unter: https://inoti.fyi

Kontakt

Sudheendra Raghav NEELA

Dipl.-Ing. BTech
TU Graz | Institute of Information Security
Tel.: +43 316 873 5540
sudheendra.neelanoSpam@tugraz.at

Daniel GRUSS
Univ.-Prof. Dipl.-Ing. Dr.techn. BSc
TU Graz | Institute of Information Security
Tel.: +43 316 873 5544
daniel.grussnoSpam@tugraz.at

https://www.tugraz.at/news/artikel/file-notification-windows-linux-android-macos-angriffe