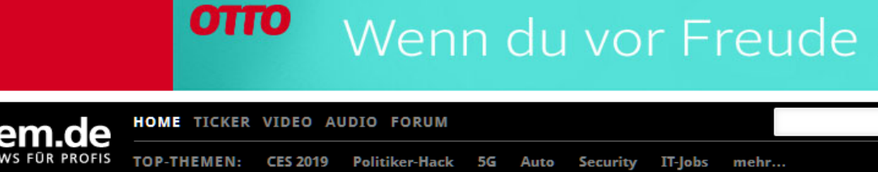
LOGITECH OPTIONS

Logitech-Software ermöglicht Ausführung von schädlichem Code

In einer Software zur Konfiguration von Logitech-Tastaturen und Mäusen klafft ein riesiges Sicherheitsloch. Nutzer von Logitech Options sollten es vorerst deinstallieren: Bisher gibt es keinen Fix.

12. Dezember 2018, 16:45 Uhr, Hanno Böck



LOGITECH OPTIONS

Logitech-Software ermöglicht Ausführung von schädlichem Code

In einer Software zur Konfiguration von Logitech-Tastaturen und Mäusen klafft ein riesiges Sicherheitsloch. Nutzer von Logitech Options sollten es vorerst deinstallieren: Bisher gibt es keinen Fix.

12. Dezember 2018, 16:45 Uhr, Hanno Böck

(Bild: Wikimedia Commons / Yannik

Gefährliche Konfigurationssoftware: Nutzer von Logitech Options sollten die Software besser deinstallieren.

Tavis Ormandy von Googles Project Zero hat in Logitech Options eine schwere Sicherheitslücke entdeckt. Die Software öffnet einen lokalen Websockets-Port, der ohne Authentifizierung Befehle entgegennimmt. Damit kann man beispielsweise Tastatureingaben simulieren und somit potentiell Code auf dem System ausführen.

Ormandy hatte sich die Software installiert, da er die Buttons seiner Maus unter Windows konfigurieren wollte. Dafür musste er die knapp 150 Megabyte große Software Logitech Options installieren. Nach der Installation wird die Software automatisch bei jedem Systemstart von Windows aufgerufen.

Software stürzt bei falschen Daten ab

Auf dem lokalen TCP-Port 10134 läuft anschließend ein Websockets-Service. Webseiten können mit diesem Service kommunizieren. Laut Ormandy lassen sich an den Service JSON-codierte Befehle schicken, deren Korrektheit wird aber nicht geprüft. Somit ist es sehr leicht möglich, den Service abstürzen zu lassen, indem man Daten mit unerwarteten Datentypen hinschickt.

Doch Ormandy fand ein noch viel größeres Problem: Der Service akzeptiert Befehle von beliebigen Webseiten. Er prüft die Herkunft der gesendeten Befehle, die sogenannte Origin, nicht. Das bedeutet, dass jede beliebige Webseite Befehle an den Websockets-Port schicken kann.

Damit die Befehle akzeptiert werden, müssen diese zwar die Prozess-ID des jeweiligen Services kennen. Doch diese ID ist nur wenige Stellen lang und lässt sich daher sehr schnell durch simples Ausprobieren herausfinden.

Auch neue Version betroffen

Ormandy schreibt, dass er sich im September mit Logitech-Entwicklern getroffen hat, um ihnen das Problem zu erläutern. Sie hätten ihm versichert, dass sie das Problem verstanden hätten und dass sie eine Prüfung der Origin und der korrekten Datentypen einbauen wollen. Doch laut Ormandy hat auch die jüngste Version von Logitech Options, die am 1. Oktober veröffentlicht wurde, dieselben Probleme.

Wir haben Logitech um eine Stellungnahme gebeten, eine Antwort haben wir bisher nicht erhalten. Anwendern von Logitech-Produkten sollten die Options-Software vorerst umgehend deinstallieren, da sie ansonsten einem hohen Risiko ausgesetzt sind.

Nachtrag vom 14. Dezember 2018, 10:54 Uhr

Logitech bietet auf seiner Webseite inzwischen ein Update an. Laut dem Twitteraccount der Firma sind die Sicherheitslücken behoben, auf der Webseite steht dazu jedoch nichts. Wir haben bei Tavis Ormandy nachgefragt und ihn gebeten zu prüfen, ob die Lücken tatsächlich geschlossen sind. Sobald wir eine Antwort haben, werden wir dies nachtragen. ■

Themenseiten:
Logitech, Eingabegerät, Maus, Project Zero, Sicherheitslücke, Tastatur, Treiber, Websockets, Applikationen, PC-Hardware, Security

Zu den Kommentaren springen

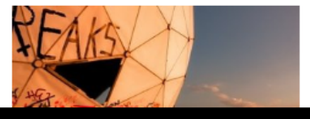
Weitere interessante Artikel

DASH-BUTTONS: GERICHT VERBIETET AMAZONS EINKAUFS...

PADRONE ANGESEHEN: EINE MAUSALTERNATIVE, DIE...

HYPERLOOPTT: HAMBURG SOLL EINEN HYPERLOOP BEKOMMEN

RASPBERRY PI: RASPBIAN BEKOMMT HARDWAREBE...



Golem.de benutzt Cookies, um seinen Lesern das beste Webseiten-Erlebnis zu ermöglichen. Außerdem werden teilweise auch Cookies von Diensten Dritter gesetzt. Weiterführende Informationen erhalten Sie in der Datenschutzerklärung von Golem.de.
Ich habe verstanden!