ÖSTERREICHISCHES BUNDESHEER
IKT & Cybersicherheitszentrum
MilCySihZ

WARNMELDUNG
Wireless Logitech-Geräte

Wien, am 09.07.2019

Sachlage

Im Rahmen einer Forschungsarbeit wurden Anfang Juni mehrere Schwachstellen in Wireless Protokollen entdeckt [1]. Verwundbar sind alle Logitech-Geräte, die mit der Unifying-Funktechnik arbeiten. Logitech liefert die betroffenen „Unifying"-USB-Empfänger seit 2009 bis heute mit kabellosen Tastaturen und Mäusen aus. „Unifying" kommt sowohl bei preiswerten Einsteigerprodukten als auch bei aktuellen Spitzenmodellen zum Einsatz. Man erkennt die betroffenen USB-Receiver an einem kleinen orangefarbenen Logo (siehe Bild 1) mit einem Stern. Alle technischen Details können unter der CVE 2019-13053 gefunden werden. (s.a. Artikel von Heise [2])

Bild 1

Auswirkungen

Demnach ist die Funkkommunikation zwischen den Präsenteren und dem/n Empfänger/n aufgrund unzureichend geschützter Datenübertragung und fehlender Authentifizierungsmechanismen manipulierbar. Angreifer können Tastatureingaben fälschen und diese (in Gestalt injizierter Datenpakete) an den Zielrechner schicken ("Keystroke Injection"). Auf diese Weise könnten sie beispielsweise Schadcode installieren und letztlich die Kontrolle über das System übernehmen.

Was ist zu tun

Aufgrund der erhöhten Gefahrenlage wird ersucht die betroffenen Geräte, bis zur Lösung des Problems, **nicht zu benutzen**. Hierfür reicht es jedoch nicht das Geräte (Präsenteren/ Maus / Tastatur) selbst nicht zu benutzen, sondern **es muss der Empfänger (siehe Bild 1) vom Gerät getrennt werden**! IKT&CySihZ arbeitet, in direkter Zusammenarbeit mit dem Hersteller an einer raschen Behebung des Problems.

[1] www.syss.de/pentest-blog/2019/syss-2019-007-syss-2019-008-und-syss-2019-015-keystroke-injection-schv weiteren-wireless-presentern/

[2] https://www.heise.de/ct/artikel/c-t-deckt-auf-Tastaturen-und-Maeuse-von-Logitech-weitreichend-angreifb 4464149.html

ZUSAMMEN STÄRKER