Mysteriöses iPhone-Update schützt vor Mail-Schwachstelle in iOS 16

Apple veröffentlichte kürzlich eine „Ein-Fehler-Meldung". Ungewöhnlich, meint Sicherheitsexperte Paul Ducklin von Sophos. Aber einmal im Teufelskreis einer DoS-Nachrichten-Attacke, gibt es kaum einen Ausweg.

Die Anwendung Apple Mail ist solide, auf die wichtigsten Funktionen reduziert und verlässlich. Bislang, denn es scheint in der letzten Version ein ernstes Problem aufgetaucht zu sein. Apple veröffentlichte einen Security-Patch für iOS 16, der die Versionsnummer auf iOS 16.0.3 erhöht und fixte zugleich eine Schwachstelle speziell für Mail.

Offiziell heißt es:
Ein und nur ein Fehler ist aufgeführt:
Auswirkungen: Die Verarbeitung einer schadhaften E-Mail kann zu einem Denial-of-Service führen.
Beschreibung: Ein Problem bei der Eingabevalidierung wurde mit einer verbesserten Eingabevalidierung behoben.

Die „Ein-Fehler"- Meldung
Ein-Fehler-Meldungen von Apple – oder jedem anderen Unternehmen – sind eher die Ausnahme als die Regel. Sie scheinen genau dann gepusht zu werden, wenn es eine klare und sehr präsente Gefahr gibt, wie einen Zero-Day-Exploit oder eine Exploit-Sequenz.

Das vielleicht bekannteste letzte Notfall-Update dieser Art war der Double-Zero-Day-Fix im August 2022: Ein Patch gegen einen doppelten Angriff, der aus einer Lücke im WebKit zur Ausführung von Remote-Code (ein Weg hinein) und einer Lücke im Kernel selbst zur Ausführung von lokalem Code (ein Weg zur vollständigen Übernahme) bestand.

Derartige Fehler werden nicht nur als bekannt gegenüber Außenstehenden gelistet, sondern auch offiziell als aktiver Missbrauch eingestuft. Vermutlich, um eine Sorte Schadsoftware einzuschleusen, die alles überwachen könnte, was der Nutzer macht. Also zum Beispiel Daten ausspähen, heimlich Screenshots machen, Telefongespräche belauschen und Bilder mit der Kamera aufnehmen.

Sie haben Post, Sie haben Post, Sie haben Post…
So genannte Denial-of-Service (DoS)-Fehler werden oft als Leichtgewichte der Schwachstellen-Szene betrachtet, da sie generell Angreifern keinen Weg zu Daten ermöglichen, die sie nicht sehen sollten, oder Zugang zu Privilegien bieten, die ihnen nicht zustehen, um Schadcode eigener Wahl starten zu können.

Dennoch kann jeder DoS-Fehler schnell zu einem ernsten Problem werden, besonders wenn er immer und immer wieder passiert, sobald er erstmalig ausgelöst wurde. Solch eine Situation kann schnell in Nachrichten-Apps erwachsen, wenn der bloße Zugriff die Anwendung zum Absturz bringt, weil man normalerweise die App verwenden muss, um die problematische Nachricht zu löschen. Und wenn der Absturz schnell genug ist, hat man keine Chance, diesen „Auslöser" zu löschen. Ein Teufelskreis.

Zahlreiche Geschichten tauchten über die Jahre über iPhone „Text-of-death"-Szenarien dieser Art auf, hier eine kleine Hitliste:

- Ein Szenario im Jahr 2013, das offenbar mit dem mehrfachen Wechsel der Textrichtung zusammenhing (wenn man beispielsweise einen arabischen Text von rechts nach links in einen englischen Satz von links nach rechts einfügt).

- Ein Vorfall in 2018, verursacht durch die Anzeige einer bestimmten Zeichenkombination in Telugu (eine Sprache im Südindischen Raum).

- In 2020 ging etwas bei der Schreibweise des Wortes BAD in Urdu (Landessprache in Pakistan) schief – technisch legal; es lag es einfach an der seltsamen Schriftfolge in dieser Sprache.

Ein weiteres Problem für das, was Sicherheitsexperten oft scherzhaft als CRASH: GOTO CRASH-Fehler in Messaging-Apps bezeichnen, ist natürlich, dass andere Leute entscheiden können, wann sie dem Nutzer eine Nachricht schicken und was sie in die Nachricht schreiben. Und selbst wenn der Nutzer eine Art von automatisierter Filter-Regel in der App verwendet, um Nachrichten von unbekannten oder nicht vertrauenswürdigen Absendern zu blockieren, muss die Anwendung die Nachricht bearbeiten. Die Anwendung kann also trotzdem abstürzen und bei jedem Neustart wieder, wenn sie einfach nur versucht, eine Nachricht zu verarbeiten, die sie beim letzten Mal vorm Absturz nicht verarbeiten konnte. Man sieht, hier kann es zu keinem positiven Abschluss kommen.

Was kann der Anwender tun?
Egal, ob man sich für automatische Update entschieden hat oder nicht, sollten Nutzer folgendes tun:
Gehen Sie auf Einstellungen → Allgemein → Softwareupdate: hier schauen Sie, ob eine Fehlerbehebung angeboten wird. Wenn ja, installieren Sie sie.

Die gewünschte Version nach dem Update ist: iOS 16.0.3 oder später.

Die Tatsache, dass Apple ein Sicherheits-Patch für diesen DoS-Fehler veröffentlicht hat, lässt mutmaßen, dass ein Angreifer, der diesen Fehler findet, einen recht umfangreichen Schaden anrichten könnte. Zum Beispiel ein dann kaum nutzbares Gerät, das der Nutzer komplett löschen und neu aufsetzen müsste, um es wieder funktionsfähig zu machen.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de