Macher des Signal-Messenger hacken Spionage-Software von Cellebrite

Originalartikel

Backup

<html> <header class=„article-header“><h1 class=„articleheading“>Macher des Signal-Messenger hacken Spionage-Software von Cellebrite</h1> Uli Ries </header><figure class=„aufmacherbild“><figcaption class=„akwa-caption“>Eine Anspielung auf den Film „Hackers“ aus dem Jahr 1995: MESS WITH THE BEST, DIE LIKE THE REST. HACK THE PLANET!</figcaption></figure> Die Signal-Entwickler zeigen per Video, wie ein präpariertes iPhone die von Ermittlungsbehörden verwendete Software von Cellebrite aushebelt. „Vom Laster gefallen“ sei das Cellebrite-Kit, das die Signal-Entwickler auf Schwachstellen untersuchen konnten. Das israelische Unternehmen Cellebrite steht regelmäßig in der Kritik [1], weil seine Spionage- und Datenanalyse-Produkte in Staaten mit Demokratiedefiziten wie Weißrussland, Myanmar oder den Vereinigten Arabischen Emiraten zum Einsatz kommen. <h3 class=„subheading“ id=„nav_spionage_softwar0“>Spionage-Software mit Schwachstellen</h3> In einem bemerkenswerten Blog-Beitrag [2] beschreibt Signal-Erfinder Moxie Marlinspike, wie schlecht es um die Sicherheit der von Ermittlungsbehörden weltweit verwendeten Cellebrite-Software [3] bestellt ist. Unter anderem befänden sich aus dem Jahr 2012 stammende und von entsprechend vielen Sicherheitslücken geplagte DLLs des Open-Source-Video-Encoders ffmpeg in der UFED genannten Windows-Anwendung des Anbieters von Spionagesoftware. Hingegen fänden sich keine der ansonsten in der Software-Industrie üblichen Anti-Exploit-Mechanismen in der Applikation. <h3 class=„subheading“ id=„nav_hack_the_planet_1“>Hack the planet</h3> Nachdem sämtliche von UFED und der ebenfalls zum Cellebrite-Paket gehörenden Windows-Anwendung Physical Analyzer zu parsende Files nicht vertrauenswürdig sind und unvorhergesehene Formate enthalten können, führt das laut Marlinspike leicht zu Speicherkorrumpierungen. In einem kurzen, mit Ausschnitten aus dem Kultfilm „Hackers“ angereicherten Video im Blog-Beitrag zeigen die Signal-Macher die Auswirkungen solcher Bugs: Während des Parsens eines iPhone-Backups öffnet sich ein Windows-Hinweisfenster mit dem Inhalt „Mess with the best, die like the rest! Hack the planet!“ – eine weitere Anspielung auf „Hackers“.

Auslöser für die Meldung war offenbar eine auf dem iPhone gespeicherte, speziell präparierte Datei, das den Parser aus dem Tritt brachte. Die im Video gezeigte Version 7.40 von UFED ist seit Ende November 2020 im Umlauf. Derzeit aktuell ist Version 7.44. Laut der Aussage der Signal-Entwickler sei das Gezeigte nur die Spitze des Eisbergs. Man könne dank der Schwachstellen beliebigen Code auf dem Windows-Rechner ausführen. So sei beispielsweise das Ausschleusen von Daten nach draußen möglich oder die Manipulation sämtlicher von der Cellebrite-Software erzeugten Reports. Dies gelte für bereits vorhandene Berichte und künftig erstellte. Träfe dies tatsächlich zu, wären die Reports als Beweismittel vor Gericht untauglich. <h3 class=„subheading“ id=„nav_vergiftete2“>Vergiftete Beigabe</h3> Am Ende des Blogbeitrags bringen die Signal-Macher die Giftpille ins Spiel: Kommende Signal-Versionen würden auf einzelnen Geräten regelmäßig Dateien nachladen und im App-Speicher ablegen. Die Dateien dienten „lediglich der Optik“ und hätten sonst keine Funktion innerhalb der Messenger-App. Signal spielt offensichtlich darauf an, mittels dieser Dateien Exploits für die Cellebrite-Software zu verteilen. Man habe diverse dieser „optisch ansprechenden“ Dateien im Fundus und werde diese nach und nach ausspielen. UPDATE 22.04.2021 11:30 Uhr: Aufgrund von Korrektheit: Überwachungs-Software durch Spionage-Software ersetzt. () <hr /> URL dieses Artikels:
<small><code>https://www.heise.de/-6024421</code></small> Links in diesem Artikel:
<small><code>[1] https://www.heise.de/meldung/iPhone-Hacking-Tools-auf-eBay-gesichtet-4324268.html</code></small>
<small><code>[2] https://signal.org/blog/cellebrite-vulnerabilities/</code></small>
<small><code>[3] https://www.heise.de/meldung/Entsperrhack-FBI-will-weitere-iPhones-und-iPods-knacken-3159476.html</code></small>
<small><code>[4] mailto:des@heise.de</code></small>
 Copyright © 2021 Heise Medien </html>