STATEMENT ZUM FAXPLOIT

Produkte der Ferrari electronic AG nicht betroffen

No. 2018-08

Revision 1.2

Statement | Ferrari electronic AG

Ferrari electronic

Statement zum Faxploit

Eins vorweg: Der gefundene Exploit ist ein neuer ernst zu nehmender Angriffsvektor. Die Produkte der Ferrari electronic sind jedoch **nicht** von der gefundenen Schwachstelle **betroffen**.

Um diese Angriffsmöglichkeit auszunutzen, ist es notwendig ein mit Angriffscode präpariertes JPEG zu übertragen und als Empfänger auch entsprechend auszuwerten. Es wird hier eine Schwachstelle der in den HP-MFPs eingesetzten JPEG-Library ausgenutzt.

Das JPEG-Format wird von OfficeMaster weder auf der Empfangsseite noch auf der Sendeseite unterstützt. D.h. Benutzer können weder Verursacher noch Opfer sein, wenn OfficeMaster Produkte eingesetzt werden.

Der Angriff auf die MFPs hat nichts mit Fax selbst zu tun. Der Exploit könnte genauso über SMTP oder eine Dateifreigabe erzielt werden. Fax dient hier lediglich als Transportmedium. Bei den eingesetzten Multifunktionsdruckern kann einfach der JPEG-Empfang deaktiviert oder aber das von HP zur Verfügung gestellte Sicherheitsupdate eingespielt werden und dieser Angriffsvektor ist geschlossen.

Was wurde entdeckt?

Das Faxprotokoll entwickelt sich seit ca. 40 Jahren kontinuierlich weiter und hat in dieser Zeit auch Modi erhalten, die es erlauben, direkt Dokumente im Format JPEG (T.81) zu übertragen. Bei der Suche nach der Schwachstelle im Faxprotokoll wurde festgestellt, dass ein Angriff auf die zumeist eingesetzten Protokolle T.4 und T.6 nicht durchgeführt werden konnte. (“We checked the decompression code for T.4 and T.6 and couldn’t find any interesting vulnerabilities there.” [FEX01]) Auch die Übertragung der angesprochenen JPEGs konnte nicht korrumpiert werden. Es konnten allerdings mit Malware infizierte JPEG-Dateien übertragen werden. Auf Basis dieser Dateien wurden dann die im Experiment beschriebenen Angriffe durchgeführt.

[FEX01] https://research.checkpoint.com/sending-fax-back-to-the-dark-ages/
[FEX02] https://www.heise.de/security/meldung/Totale-Kontrolle-Multifunktions-Drucker-ueber-Fax-angreifbar-4135522.html?wt_mc=rss.ho.beitrag.rdf