



BSI-Warnung gemäß BSIG § 7

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht die vorliegende Warnung im Rahmen seines gesetzlichen Auftrags [1].

M Horse Pure 1: Schadsoftwareinfektion im Auslieferungszustand

Risikostufe [2]: 5 - sehr hoch

1 Sachverhalt

Das M-Horse Pure 1 ist ein Android-Smartphone des Herstellers M-Horse. Es ist bereits im Auslieferungszustand mit einer Schadsoftware infiziert.

2 Auswirkung

BSI-eigene Analysen [3] haben ergeben, dass eine vorinstallierte, bösartige App Geräteinformationen sammelt und diese an ein entferntes System sendet. Darüber hinaus meldet die Schadsoftware die Installation und Deinstallation von Apps durch den Benutzer an einen Server. Hierbei handelt es sich um eine Variante des in [4] beschriebenen Schadprogramms. Zusätzlich verfügt die genannte App über die Möglichkeit, unbemerkt über ein Netzwerk zu kommunizieren und bietet eine Hintertür zur Fernsteuerung des Geräts durch einen Angreifer an. Über diese sind unter anderem der Download sowie die Installation weiterer Schadprogramme möglich. Die Installation weiterer Programme oder die Fernsteuerung des Gerätes konnte bisher nicht beobachtet werden.

3 Betroffene Systeme

M-Horse Pure 1

Build-Nr: V3G23HB.JHM.M_HORSE.HB.HJ.PA.1118.V3.04

4 Handlungsempfehlung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt, von einer Nutzung des Gerätes abzusehen.

Falls vorhanden, sollten gesetzliche Gewährleistungsansprüche gegenüber dem Händler geltend gemacht werden.

Anwender können ihre Betroffenheit feststellen, indem sie prüfen, ob auf Ihrem Gerät die Firmware-Version der oben angegebenen Build-Nr. entspricht. Diese lässt sich unter "Einstellungen" → "Über das Telefon" (Android-Systemeinstellung) anzeigen. Zum Zeitpunkt der Prüfung war vom Hersteller nur die Firmware V3.04 verfügbar. Es wurde vom BSI zusätzlich eine im Internet verfügbare Firmware mit der Bezeichnung V3G23HB.JHM.M_HORSE.HB.HJ.PA.1212.V3.05 geprüft, bei der aber weiterhin eine Betroffenheit festgestellt werden konnte.

5 Referenzen

- [1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)
https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html
- [2] Darstellung Risikostufen
<https://www.cert-bund.de/risk>
- [3] BSI-Pressemitteilung
<https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/bsi-warnung-smartphones-060619.html>
- [4] Sophos Blog
<https://news.sophos.com/en-us/2018/10/02/the-price-of-a-cheap-mobile-phone-may-include-your-privacy/>