Warnmeldung 2018-108

05. Dezember 2018, 14:45 Uhr Bearbeiter: Conradi

Google Android

Zahlreiche kritische Schwachstellen geschlossen

Tags: Google Android

Sachverhalt

Das CERT-Bund im Bundesamt für die Sicherheit in der Informationstechnik (BSI) warnt mit Risikobewertung „4 - HOCH“ in seiner aktuellen Kurzinfo CB-K18-1140 vor zahlreichen kritischen Schwachstellen in **Google Android**. Einem entfernten, anonymen Angreifer ermöglichen diese, beliebigen Programmcode mit erhöhten Rechten auszuführen, um seine Privilegien zu erhöhen, um Informationen offenzulegen oder um einen Denial of Service Zustand herbeizuführen.

Zusätzliche Informationen zu „*BlackBerry powered by Android*“ liegen nicht vor.

Weitere Details finden Sie unter https://www.cert-bund.de/advisoryshort/CB-K18-1140 .

Bewertung

Google Android ist ein – in den Hauptbestandteilen quelloffenes – Betriebssystem sowie eine Software-Plattform für mobile Endgeräte. Diese werden von der „*Open Handset Alliance*“ entwickelt, deren Hauptmitglied Google ist. Das Betriebssystem nutzt den Linux-Kernel. Google Android ist auf mobilen Endgeräten, wie Smartphones oder Tablets, – nicht zuletzt aufgrund günstiger Preise für die Endgeräte – weit verbreitet.

Das CERT-Bund im BSI stuft die Schwachstellen mit seiner zweithöchsten Risikobewertung „*4 - HOCH*“ ein. Das CERT-Hessen schließt sich dieser Einschätzung an.

Empfehlung von Maßnahmen

Falls Sie in Ihrem Verantwortungsbereich mobile Endgeräte mit dem Betriebssystem Google Android (z. B. Smartphones, Tablets, etc.) verwenden, empfiehlt Ihnen

das CERT-Hessen diese zur Gewährleistung eines sicheren IT-Betriebs nur in der jeweils aktuellsten Betriebssystemversion und nur mit dem jeweils aktuellsten Sicherheitsupdate („Patchlevel“) zu betreiben. Hierbei wird vorausgesetzt, dass die von der „*Open Handset Alliance*“ in der Regel monatlich für Google Android bereitgestellten Sicherheitsupdates („Patchlevel“) über die gesamte wirtschaftliche Nutzungsdauer der Geräte zeitnah und Typ-kompatibel durch den jeweiligen Hersteller bereit gestellt werden. Aus diesem Grund sieht das CERT-Hessen die Bereitstellung von Sicherheitsupdates beispielsweise nur einmal pro Quartal kritisch.

Mit Blick auf das hier aktuell vorliegende Risiko sollte die nun anstehende Aktualisierung Ihrer mobilen Endgeräte – unter Berücksichtigung Ihrer vor Ort aktuell gültigen Prüf- und Freigabenprozesse für Software – zeitnah erfolgen.

Endgeräte, für die der jeweilige Hersteller keine Sicherheitsupdates (mehr) anbietet, stellen ein erhebliches Sicherheitsrisiko dar. Das CERT-Hessen empfiehlt Ihnen, solche Geräte auszutauschen. Auch im privaten Umfeld sollte – unter Berücksichtigung der konkreten Verwendung des jeweiligen Endgeräts – sorgfältig abgewogen werden, ob die Verwendung eines Endgerätes ohne regelmäßige Sicherheitsupdates und damit mit zahlreichen, veröffentlichten und kritischen Schwachstellen noch mit dem persönlichen Sicherheitsbedarf vereinbar ist.

Ihr CERT-Hessen

Kurzfassung: Bedeutung der Traffic Light Protocol-Einstufungen

TLP-Stufen

Stufe	Bedeutung	Bestimmungen
TLP-White	Unbegrenzt	Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-White ohne Einschränkungen frei weitergegeben werden.
TLP-Green	Organisations-übergreifende Verteilung	Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
TLP-Amber	Organisationsinterne Verteilung	Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig". Der Ersteller der Information muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.
TLP-Red	Persönlich, nur für benannte Empfänger	**TLP-Red-Informationen** sind auf den Kreis der Anwesenden in einer Besprechung oder einer Video-/Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden Informationen der Stufe TLP-Red mündlich oder persönlich übergeben.

Eine ausführliche Erläuterung zum Traffic-Light-Protokoll finden Sie im Dokument „CERT-Verpflichtung-TLP.pdf" unter http://www.cert.hessen.de

Kontaktdaten:

Hessisches Ministerium des Innern und für Sport

CERT HESSEN

Friedrich-Ebert-Allee 12
65185 Wiesbaden

Telefon (Sammelruf): +49 (611) 340 30 30
Fax: +49 (611) 353 1919

E-Mail: cert-hessen@hmdis.hessen.de

Website: http://www.cert.hessen.de/

Bearbeiter:

Jens Conradi
Telefon (persönlich): +49 (611) 353 1988
E-Mail: Jens.Conradi@hmdis.hessen.de

Detlef Hartel
Telefon (persönlich): +49 (611) 353 1985
E-Mail: Detlef.Hartel@hmdis.hessen.de

Martina Ohlenmacher
Telefon (persönlich): +49 (611) 353 1975
E-Mail: Martina.Ohlenmacher@hmdis.hessen.de