N-CERT Niedersächsisches Computer Emergency Response Team

Niedersachsen

Advisory 2016-1067

Google Android: Mehrere Schwachstellen

Datum: 2016-08-02
Stand: 2016-08-02

Risiko gesamt

Angriffswahrscheinlichkeit: mittel
Potentielle Schadenshöhe: hoch

Plattformen

- Android

betroffene Produkte

- Google Android 4.4.4
- Google Android 5.0.2
- Google Android 5.1.1
- Google Android 6.0
- Google Android 6.0.1

Angriff

Ein entfernter, anonymer Angreifer kann mehrere Schwachstellen in Google Android ausnutzen, um beliebigen Programmcode mit Kernel-/Applikationsrechten auszuführen, um seine Rechte zu erweitern, um einen Denial of Service Zustand herbeizuführen und um Informationen offenzulegen.

Beschreibung

Das Android Betriebssystem von Google ist eine quelloffene Plattform für mobile Geräte. Die Basis bildet der Linux-Kernel.

CVE-2012-6701, CVE-2014-9863, CVE-2014-9864, CVE-2014-9865, CVE-2014-9866, CVE-2014-9867, CVE-2014-9868, CVE-2014-9869, CVE-2014-9870, CVE-2014-9871, CVE-2014-9872, CVE-2014-9873, CVE-2014-9874, CVE-2014-9875, CVE-2014-9876, CVE-2014-9877, CVE-2014-9878, CVE-2014-9879, CVE-2014-9880, CVE-2014-9881, CVE-2014-9882, CVE-2014-9883, CVE-2014-9884, CVE-2014-9885, CVE-2014-9886, CVE-2014-9887, CVE-2014-9888, CVE-2014-9889, CVE-2014-9890, CVE-2014-9891, CVE-2014-9892, CVE-2014-9893, CVE-2014-9894, CVE-2014-9895, CVE-2014-9896, CVE-2014-9897, CVE-2014-9898, CVE-2014-9899, CVE-2014-9900, CVE-2014-9901, CVE-2014-9902, CVE-2014-9903, CVE-2014-9904, CVE-2015-1593, CVE-2015-2686, CVE-2015-8937, CVE-2015-8938, CVE-2015-8939, CVE-2015-8940, CVE-2015-8941, CVE-2015-8942, CVE-2015-8943, CVE-2015-8944, CVE-2016-2497, CVE-2016-2504, CVE-2016-2544, CVE-2016-2546, CVE-2016-2842, CVE-2016-3672, CVE-2016-3819, CVE-2016-3820, CVE-2016-3821, CVE-2016-3822, CVE-2016-3823, CVE-2016-3824, CVE-2016-3825, CVE-2016-3826, CVE-2016-3827, CVE-2016-3828, CVE-2016-3829, CVE-2016-3830, CVE-2016-3831, CVE-2016-3832, CVE-2016-3833, CVE-2016-3834, CVE-2016-3835, CVE-2016-3836, CVE-2016-3837, CVE-2016-3838, CVE-2016-3839, CVE-2016-3840, CVE-2016-3841, CVE-2016-3842, CVE-2016-3843, CVE-2016-3844, CVE-2016-3845, CVE-2016-3846, CVE-2016-3847, CVE-2016-3848, CVE-2016-3849, CVE-2016-3850, CVE-2016-3851, CVE-2016-3852, CVE-2016-3853, CVE-2016-3854, CVE-2016-3855, CVE-2016-3856, CVE-2016-3857, CVE-2016-4482, CVE-2016-4569, CVE-2016-4578

In Google Android existieren 102 Schwachstellen im Zusammenhang mit dem Mediaserver, libjhead, system clock, framework APIs, shell, camera API, SurfaceFlinger, Wi-Fi, system UI, Bluetooth, Conscrypt, kernel networking component, Qualcomm GPU driver, Qualcomm performance component, kernel sound component, ION driver, Qualcomm bootloader, kernel performance subsystem, kernel scheduler, USB driver, Google Play services und thermal driver. Ein anonymer, entfernter Angreifer kann diese Schwachstellen ausnutzen, um beliebigen Programmcode mit Kernel-/Applikationsrechten auszuführen, um seine Rechte zu erweitern, um einen Denial of Service Zustand herbeizuführen oder um Informationen offenzulegen. Zur erfolgreichen Ausnutzung mancher dieser Schwachstellen muss der Angreifer den Benutzer dazu bringen eine modifizierte Datei zu öffnen.

CVSSv2
AV:N/AC:M/Au:N/C:C/I:C/A:C/E:U/RL:OF
Base Score: 9.3
Temporal Score: 6.9

Empfehlung

Google stellt Updates zur Verfügung. Bitte installieren Sie die aktuelle Version unter Berücksichtigung Ihrer Betriebssystemumgebung
https://source.android.com/security/bulletin/2016-08-01.html

BlackBerry stellt Updates zur Verfügung. Bitte installieren Sie die aktuelle Version unter Berücksichtigung Ihrer Betriebssystemumgebung
http://support.blackberry.com/kb/articleDetail?articleNumber=000038360

Informationen

Android Security Bulletin - August 2016 vom 2016-08-01
https://source.android.com/security/bulletin/2016-08-01.html

BlackBerry powered by Android Security Bulletin - August 2016
http://support.blackberry.com/kb/articleDetail?articleNumber=000038360

Referenzen

CVE:CVE-2012-6701
CVE:CVE-2014-9863
CVE:CVE-2014-9864
CVE:CVE-2014-9865
CVE:CVE-2014-9866
CVE:CVE-2014-9867
CVE:CVE-2014-9868
CVE:CVE-2014-9869
CVE:CVE-2014-9870
CVE:CVE-2014-9871
CVE:CVE-2014-9872
CVE:CVE-2014-9873
CVE:CVE-2014-9874
CVE:CVE-2014-9875
CVE:CVE-2014-9876
CVE:CVE-2014-9877
CVE:CVE-2014-9878
CVE:CVE-2014-9879
CVE:CVE-2014-9880

CVE:CVE-2014-9881
CVE:CVE-2014-9882
CVE:CVE-2014-9883
CVE:CVE-2014-9884
CVE:CVE-2014-9885
CVE:CVE-2014-9886
CVE:CVE-2014-9887
CVE:CVE-2014-9888
CVE:CVE-2014-9889
CVE:CVE-2014-9890
CVE:CVE-2014-9891
CVE:CVE-2014-9892
CVE:CVE-2014-9893
CVE:CVE-2014-9894
CVE:CVE-2014-9895
CVE:CVE-2014-9896
CVE:CVE-2014-9897
CVE:CVE-2014-9898
CVE:CVE-2014-9899
CVE:CVE-2014-9900
CVE:CVE-2014-9901
CVE:CVE-2014-9902
CVE:CVE-2014-9903
CVE:CVE-2014-9904
CVE:CVE-2015-1593
CVE:CVE-2015-2686
CVE:CVE-2015-8937
CVE:CVE-2015-8938
CVE:CVE-2015-8939
CVE:CVE-2015-8940
CVE:CVE-2015-8941
CVE:CVE-2015-8942
CVE:CVE-2015-8943
CVE:CVE-2015-8944
CVE:CVE-2016-2497
CVE:CVE-2016-2504
CVE:CVE-2016-2544
CVE:CVE-2016-2546
CVE:CVE-2016-2842
CVE:CVE-2016-3672
CVE:CVE-2016-3819
CVE:CVE-2016-3820
CVE:CVE-2016-3821
CVE:CVE-2016-3822
CVE:CVE-2016-3823
CVE:CVE-2016-3824
CVE:CVE-2016-3825
CVE:CVE-2016-3826
CVE:CVE-2016-3827
CVE:CVE-2016-3828
CVE:CVE-2016-3829
CVE:CVE-2016-3830
CVE:CVE-2016-3831
CVE:CVE-2016-3832

CVE:CVE-2016-3833
CVE:CVE-2016-3834
CVE:CVE-2016-3835
CVE:CVE-2016-3836
CVE:CVE-2016-3837
CVE:CVE-2016-3838
CVE:CVE-2016-3839
CVE:CVE-2016-3840
CVE:CVE-2016-3841
CVE:CVE-2016-3842
CVE:CVE-2016-3843
CVE:CVE-2016-3844
CVE:CVE-2016-3845
CVE:CVE-2016-3846
CVE:CVE-2016-3847
CVE:CVE-2016-3848
CVE:CVE-2016-3849
CVE:CVE-2016-3850
CVE:CVE-2016-3851
CVE:CVE-2016-3852
CVE:CVE-2016-3853
CVE:CVE-2016-3854
CVE:CVE-2016-3855
CVE:CVE-2016-3856
CVE:CVE-2016-3857
CVE:CVE-2016-4482
CVE:CVE-2016-4569
CVE:CVE-2016-4578

Disclaimer

Die Angriffswahrscheinlichkeit wird durch den Nutzen Dritter (Motivation), den notwendigen Aufwand und die Möglichkeiten für einen Angriff bestimmt. Die Schadenshöhe wird durch den Aufwand zur Behebung des Schadens und die möglicherweise mittelbaren Auswirkungen des Schadens auf Geschäftsprozesse bestimmt. Es werden "worst case" Annahmen zugrunde gelegt.

Die veröffentlichten Informationen beruhen auf vertrauenswürdigen und zuverlässigen Quellen oder sind überprüft worden. Für die Vollständigkeit, Genauigkeit und inhaltliche Richtigkeit der Informationen wird nur insoweit eine Haftung übernommen, als grobe Fahrlässigkeit oder Vorsatz eine Haftung begründen. Jede darüber hinausgehende Haftung, insbesondere für mögliche Schäden, die durch den Gebrauch oder die Nichtverwertbarkeit der Informationen entstehen, wird ausgeschlossen.