Starred by 20 users

Owner: amdz@google.com
User never visited

CC: apvi-monorail-admins@google.com

Status: Fixed *(Closed)*

Components: MultiplePartners

Modified: Dec 7, 2022

ReleaseDate: 2022-11-30

Type-Defect
Disclosed
Deadline-Other
Finder-ŁukaszSiewierski
Reported-2022-May-13
Partner-Multiple

Issue 100: Platform certificates used to sign malware

Reported by antho...@google.com on Fri, Nov 11, 2022, 5:01 PM GMT+1 Project Member

Description #3 by antho...@google.com (Nov 30, 2022)

OVERVIEW

Multiple platform certificates are being used to sign malware.

TECHNICAL DETAILS

A platform certificate is the application signing certificate used to sign the "android" application on the system image. The "android" application runs with a highly privileged user id - android.uid.system - and holds system permissions, including permissions to access user data. Any other application signed with the same certificate can declare that it wants to run with the same user id, giving it the same level of access to the Android operating system.

Listed below are the SHA256 hashes of the platform signing certificates and the SHA256 hashes of correctly signed malware using the platform certificate. In some cases, when multiple samples of malware were found, only one representative sample is listed.

Certificate SHA256: 2464ddfefa071f268ea7667123df05ead2293272ff2a64d9cee021c38b46c6af
Malware sample SHA256: e4e28de8ad3f826fe50a456217d11e9e6a80563b35871ac37845357628b95f6a

Certificate SHA256: 2bfa22964760a25d99ab9a14910e44fe2063b51d5b4ac2e4282573ce94996aa3
Malware sample SHA256: 5c173df9e86e959c2eadcc3ef9897c8e1438b7a154c7c692d0fe054837530458

Certificate SHA256: 34df0e7a9f1cf1892e45c056b4973cd81ccf148a4050d11aea4ac5a65f900a42
Malware sample SHA256: b1f191b1ee463679c7c2fa7db5a224b6759c5474b73a59be3e133a6825b2a284

Certificate SHA256: 369c38b18401ea16785f11720e37d7a2bc5a4d209e76955c0858ea469ad62fdf
Malware sample SHA256: 19c84a2386abde0c0dae8661b394e53bf246f6f0f9a12d84cfc7864e4a809697

Certificate SHA256: 4274243d7a954ac6482866f0cc67ca1843ca94d68a0ee53f837d6740a8134421
Malware sample SHA256: 0251beceeffbf4bf90eaaad27c147bb023388817d9fbec1054fac1324c6f8bf

Certificate SHA256: 5304915c4bb7baca28776231993996fde1baffcbbe6500fb0fc7f2d3a2888cb7
Malware sample SHA256: c612917d68803efbd2f0e960ade1662be9751096afe0fd81cee283c5a35e7618

Certificate SHA256: 9200c550f2374706eff37e3a8674bc03aeba8b25c052de638972ab94365af0a2
Malware sample SHA256: 6792324c1095458d6b78e92d5ae003a317fe3991d187447020d680e99d9b6129

Certificate SHA256: 9fc510e167d8d312e758273285414e77edac9fed944741f5682be92501f095d4
Malware sample SHA256: 091733658c7a32f4673415b11733ae729b87e2a2540c87d08ba9adf7bc62d7ed

Certificate SHA256: a7a0e10a61a5af93624376df60e9def9436358f50aa6174e5423633b856e2be1
Malware sample SHA256: 5aaefc5b4fb1e1973832f44ba2d82a70106d3e8999680df6deed3570cd30fb97

Certificate SHA256: b01dcea669eefdd991fc6a24678a8b6e6a6d0ad8986950328c69d0eea1dec0d5
Malware sample SHA256: 32b9a33ad3d5a063cd4f08e0739a6ce1e11130532fd0b7e13a3a37edaf9893eb

IMPACT

Applications signed with the platform certificate may declare that they want to share uid with the "android" application, giving them the same set of permissions without user input.

SUGGESTED ACTION
All affected parties should rotate the platform certificate by replacing it with a new set of public and private keys. Additionally, they should conduct an internal investigation to find the root cause of the problem and take steps to prevent the incident from happening in the future.

We also strongly recommend minimizing the number of applications signed with the platform certificate, as it will significantly lower the cost of rotating platform keys should a similar incident occur in the future.

NOTES
All affected parties were informed of the findings and have taken remediation measures to minimize the user impact.

Comment 1 Deleted

Comment 2 Deleted

Comment 3 Deleted

Comment 4 by antho...@google.com on Wed, Nov 30, 2022, 7:07 PM GMT+1 Project Member

Description was changed.

Comment 5 by antho...@google.com on Wed, Nov 30, 2022, 7:10 PM GMT+1 Project Member

Description was changed.

Comment 6 by antho...@google.com on Wed, Nov 30, 2022, 7:14 PM GMT+1 Project Member

Labels: -Restrict-View-Google Disclosed

Comment 7 Deleted

Comment 8 by antho...@google.com on Fri, Dec 2, 2022, 5:17 PM GMT+1 Project Member

OEM partners promptly implemented mitigation measures as soon as we reported the key compromise. End users will be protected by user mitigations implemented by OEM partners. Google has implemented broad detections for the malware in Build Test Suite, which scans system images. Google Play Protect also detects the malware. There is no indication that this malware is or was on the Google Play Store. As always, we advise users to ensure they are running the latest version of Android.

-The Android Security Team

Comment 9 by thx77...@gmail.com on Fri, Dec 2, 2022, 5:27 PM GMT+1

@Android Security Team - I'm confused. If your recommendation is to advise users to ensure they are running the latest version of Android, why hasn't there been a security update released since this event?

Comment 10 by antho...@google.com on Fri, Dec 2, 2022, 6:13 PM GMT+1 Project Member

OEMs have mitigated the issues above in previous updates. A new security update from Android is not required to mitigate these issues. Ensuring your device is running the latest version of Android is a general best security practice for users.

Comment 11 by golds...@pbgc.gov on Mon, Dec 5, 2022, 6:00 PM GMT+1

Looking to understand the potential organizational impact - were the malicious applications available for download via the Google Play Store or only via sideloading?

Comment 12 by wench...@gmail.com on Wed, Dec 7, 2022, 4:50 AM GMT+1

google play is definitely able to mark/remove apk signed with these certs, but we(end user) are not able to verify it since we have no corresponding private key to sign and upload and see if google play remove the apk

I download pixel 5 factory image and print cert of settings.apk, it's not on the list, pixel 5 is safe

$ apksigner verify --print-certs priv-app/SettingsGoogle/SettingsGoogle.apk
Signer #1 certificate SHA-256 digest: 401faefb6b1a20fbec5e1f069d955bdd42ce808046a0c727d8926a67fb141ce1