DIREKTORAT PROTEKSI INFRASTUKTUR INFORMASI
KRITIKAL NASIONAL
DEPUTI BIDANG PROTEKSI

IMBAUAN KEAMANAN

Multiple Vulnerabilities pada Android OS (2021- 05 - 01 Security Patch Level Vulnerabilities)

TLP:WHITE

PENDAHULUAN

Google telah merilis *security patch level* untuk Android yaitu versi 2021-05-01. Beberapa kerentanan telah ditemukan pada *security patch* tersebut, dan yang paling berbahaya memungkinkan dapat dilakukannya eksekusi kode jarak jauh (*remote code execution*) [1]. Sistem operasi Android dikembangkan oleh Google untuk perangkat *mobile*, termasuk namun tidak terbatas pada *smartphone, tablet,* dan *smartwatch.* Dampak paling berbahaya dari eksploitasi kerentanan ini adalah dapat memungkinkan eksekusi kode jarak jauh (*remote code execution*) untuk memperoleh hak akses terhadap suatu aplikasi. Bergantung pada hak aksesnya, penyerang dapat menginstal program, mengubah atau menghapus data, serta membuat akun baru dengan hak akses penuh sebagai administrator. Dampak lainnya adalah *privilege elevation* dan *information disclosure*. Penilaian tingkat serangan dilihat dari dampak eksploitasi kerentanan pada perangkat terdampak, dengan asumsi *platform* dan mitigasi layanan dimatikan dengan tujuan pengembangan atau jika berhasil dilakukan *bypass*. *Source code patch* untuk kerentanan tersebut telah dikeluarkan dan dapat diakses pada *Android Open Source Project* (AOSP) *repository* [2].

RISIKO

Sistem operasi android digunakan secara luas, baik untuk penggunaan individu, bisnis, maupun pemerintahan. Berdasarkan lingkup penggunanya, risiko yang ditimbulkan akibat eksploitasi kerentanan ditunjukkan pada Tabel 1 berikut.

Tabel 1. Risiko Eksploitasi Kerentanan

Pengguna	Skala	Tingkat Risiko
Pemerintah	Besar dan Menengah	Tinggi
	Kecil	Tinggi
Bisnis	Besar dan Menengah	Tinggi
	Kecil	Tinggi
Individu	-	Rendah

RINCIAN TEKNIS KERENTANAN

Sistem yang terdampak kerentanan ini adalah Android 8.1, 9, 10, dan 11. Kerentanan dikelompokkan berdasarkan komponen terdampak, sebagai berikut:

Framework

Kerentanan memungkinkan aplikasi lokal yang berbahaya melakukan *bypass* terhadap perlindungan sistem operasi yang mengisolasi data aplikasi dari aplikasi lain.

CVE	*Reference*	*Type*	*CVSS v3 Score*	*Severity*	*Updated AOSP version*
CVE-2019-2219	A-119041698	*Information Disclosure*	4,7 CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N	*High*	11

Komponen Kernel

Kerentanan pada bagian ini akan memungkinkan penyerang lokal melakukan *bypass* terhadap persyaratan interaksi pengguna untuk memperoleh akses terhadap *permission* tambahan.

CVE	*Reference*	*Type*	*Score/ Vector CVSS v3*	*Severity*	*Component*
CVE-2020-29661	A-175451802 Upstream kernel	*Elevation of Privilege*	7,8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	*High*	TTY

AMLogic

Kerentanan akan berdampak pada komponen AMLogic. Detail informasi kerentanan dan *severity* belum tersedia dan akan diperbaharui oleh AMLogic.

CVE	*References*	*Severity*	*Component*
CVE-2021-0467	A-174490700*	*Critical*	bootROM

Komponen ARM

Kerentanan akan berdampak pada komponen ARM. Detail informasi kerentanan dan *severity* belum tersedia dan akan diperbaharui oleh ARM.

CVE	*References*	*Severity*	*Component*
CVE-2021-28663	A-174259860*	*High*	Mali
CVE-2021-28664	A-174588870*	*High*	Mali

5/7/2021

Komponen MediaTek

Kerentanan akan berdampak pada komponen MediaTek. Detail informasi kerentanan dan *severity* belum tersedia dan akan diperbaharui oleh MediaTek.

CVE	*References*	*Severity*	*Component*
CVE-2021-0489	A-183464866 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0490	A-183464868 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0491	A-183461315 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0492	A-183459078 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0493	A-183461317 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0494	A-183461318 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0495	A-183459083 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0496	A-183467912 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0497	A-183461320 M-ALPS05403499*	*High*	*memory management driver*
CVE-2021-0498	A-183461321 M-ALPS05403499*	*High*	*memory management driver*

Komponen Unisoc

Kerentanan akan berdampak pada komponen Unisoc. Detail informasi kerentanan dan *severity* belum tersedia dan akan diperbaharui oleh Unisoc.

CVE	*References*	*Severity*	*Component*
CVE-2021-0324	A-175402462*	*High*	*Framework*

Komponen Qualcomm

Kerentanan akan berdampak pada komponen Qualcomm. Detail informasi kerentanan dan *severity* dapat diakses pada *Qualcomm security bulletin* atau *security alert*.

CVE	*References*	*Severity*	*Component*
CVE-2021-1891	A-179039763 QC-CR#2766242	*High*	*Audio*
CVE-2021-1905	A-178809945 QC-CR#2826864	*High*	*Display*
CVE-2021-1927	A-179040600 QC-CR#2827356	*High*	*Kernel*
CVE-2021-1906	A-178810049 QC-CR#2835082	*Moderate*	*Display*

Komponen Qualcomm *closed-source*

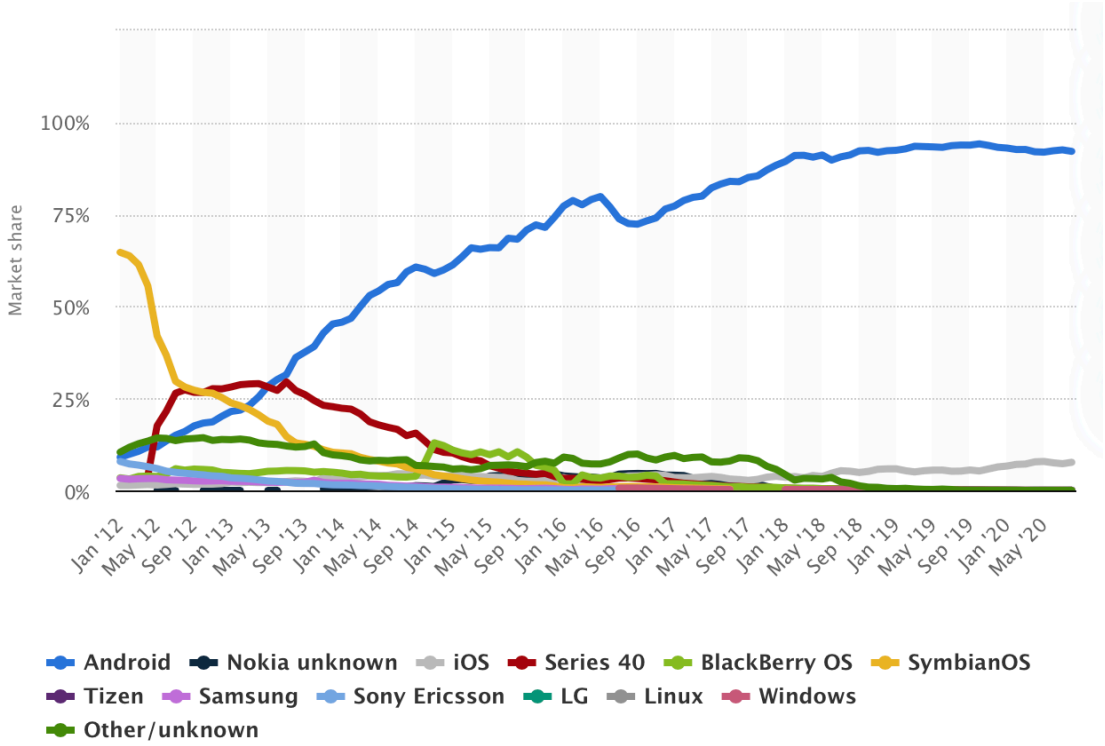
Kerentanan akan berdampak pada komponen *Qualcomm closed-source*. Detail informasi kerentanan dan *severity* dapat diakses pada *Qualcomm security bulletin* atau *security alert.*

CVE	*References*	*Severity*	*Component*
CVE-2020-11273	A-172348952*	*High*	*Closed-source component*
CVE-2020-11274	A-172348993*	*High*	*Closed-source component*
CVE-2020-11279	A-172348857*	*High*	*Closed-source component*
CVE-2020-11284	A-172348929*	*High*	*Closed-source component*
CVE-2020-11285	A-172349029*	*High*	*Closed-source component*
CVE-2020-11288	A-172348722*	*High*	*Closed-source component*
CVE-2020-11289	A-172348852*	*High*	*Closed-source component*
CVE-2021-1910	A-179039901*	*High*	*Closed-source component*
CVE-2021-1915	A-172944461*	*High*	*Closed-source component*

Dampak paling berbahaya jika eksploitasi kerentanan tersebut berhasil dilakukan adalah memungkinkan penyerang melakukan eksekusi kode jarak jauh (*remote code execution*) dalam konteks *privileged process*. Bergantung pada *privilege* yang berhubungan dengan aplikasi, penyerang akan dapat menginstal program, melihat, mengubah atau menghapus data, serta membuat akun baru dengan hak akses penuh. Jika aplikasi telah dikonfigurasi dengan hak akses yang lebih sedikit, maka dampak yang ditimbulkan akan lebih kecil.

Distribusi Pengguna Android di Indonesia (2012-2020)

Berikut distribusi penggunaan sistem operasi mobile di Indonesia berdasarkan survey pangsa pasar 2012 - 2020 yang dilakukan oleh Stastista tahun 2020 [3].



Gambar 1. Distribusi Pengguna Sistem Operasi Mobile

Gambar tersebut menunjukkan jumlah pengguna Android yang terus meningkat secara signifikan setiap tahunnya dan jauh diatas pengguna sistem operasi *mobile* lainnya. Pada Agustus 2020, Android menguasai lebih dari 90% pasar seluler di Indonesia.

LANGKAH MITIGASI DAN PENANGANAN KERENTANAN

Berikut beberapa langkah mitigasi yang dapat dilakukan pengguna Android yang terdampak, untuk meminimalisir risiko yang mungkin muncul akibat eksploitasi kerentanan:

1. Lakukan pembaruan (*update*) sesuai dengan jenis dan versi perangkat yang disediakan oleh Android [4] dan proteksi layanan seperti *Google Play Protect*

[5] .Eksploitasi kerentanan akan lebih sudah dilakukan pada versi Android yang lebih baru.

2. Dihimbau agar pengguna hanya mengunduh aplikasi dari penyedia terpercaya di *Play Store*.
3. Dihimbau agar pengguna tidak mengunjungi *website* yang tidak terpercaya atau mengunjungi tautan yang disediakan oleh sumber yang tidak dikenal/tidak terpercaya.
4. Menerapkan prinsip *least privilege* ke semua sistem operasi.

REFERENSI

[1] Center for Internet Security, "Multiple Vulnerabilities in Google Android OS Could Allow for Remote Code Execution", 4 Mei 2021. [Online]. Available: https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-google-android-os-could-allow-for-remote-code-execution_2021-060/, diakses 6 Mei 2021.

[2] Android.com, "Android Security Bulletin - May 2021". 4 Mei 2021 .[Online]. Available: https://source.android.com/security/bulletin/2021-05-01, diakses 6 Mei 2021.

[3] Statista, "Market share of mobile operating sytems in Indonesia from January 2012 to August 2020, by Operating System ". 11 Februari 2021. [Online]. Available: https://www.statista.com/statistics/262205/market-share-held-by-mobile-operating-systems-in-indonesia/, diakses 6 Mei 2021.

[4] Android.com, "Security Enhancements ".[Online]. Available: https://source.android.com/security/enhancements.

[5] Google.com, "Google Play Protect". [Online]. Available: https://developers.google.com/android/play-protect