Peran Bersama untuk Keamanan Sistem dan Data

Bahasa Indonesia

Sistem Ultrasound Lumify

PHILIPS

Isi

1 Pendahuluan..... 5

Informasi Umum..... 6

2 Kontrol terhadap Kerentanan Keamanan pada Produk Philips..... 7

Strategi Keamanan dengan Pertahanan Berlapis..... 7

Lingkungan Pengaturan..... 8

Peran Philips dalam Kemitraan Keamanan Produk..... 8

Peran Pelanggan dalam Kemitraan Keamanan Produk..... 10

Masalah Keamanan dan Panduan Keamanan..... 11

Contoh Pemeliharaan Informasi..... 13

Asumsi Tentang Lingkungan..... 14

Zona Informasi..... 14

Perangkat Lunak Perlindungan Keamanan..... 16

Pemindaian dan Pembaruan Antivirus..... 16

Cadangan dan Arsip..... 16

Prosedur Pencadangan..... 17

Rencana Pemulihan Kerusakan..... 17

4535 619 63091_A/795 * FEB 2018

Philips

4535 619 63091_A/795 * FEB 2018

Philips

1 Pendahuluan

Dokumen ini membahas keamanan pada Sistem Ultrasound Lumify. Philips menyediakan pilihan konfigurasi yang berbeda untuk Sistem Ultrasound Lumify, termasuk Bawa Perangkat Anda Sendiri (BYOD). Meskipun sistem ultrasound Philips lainnya dikirim sebagai sistem lengkap dengan pembatasan pada hal-hal yang diizinkan dan tersedia untuk sistem, perangkat host Lumify dapat disediakan, dikonfigurasi, dan dipelihara oleh organisasi perawatan kesehatan atau individu.

Pelanggan yang memenuhi syarat dapat memilih versi paket produk, yang dijual sebagai sistem lengkap (baik perangkat keras maupun perangkat lunak). Baik versi BYOD maupun versi paket, perangkat harus dikonfigurasi dan dipelihara oleh organisasi perawatan kesehatan atau individu.

Panduan ini disusun guna membantu organisasi perawatan kesehatan mengetahui hal-hal yang dapat mengganggu keamanan aplikasi Lumify Philips dan data pasien, dan untuk menekankan upaya Philips dalam memastikan bahwa panduan keselamatan tersedia untuk membantu mencegah pelanggaran keamanan.

Untuk sumber informasi keamanan sistem-ultrasound seperti buletin keamanan, FAQ, dan informasi kerentanan, lihat situs web Keamanan Produk Philips:

www.philips.com/productsecurity

Untuk informasi tentang Sistem Ultrasound Lumify, kunjungi portal Lumify:

www.philips.com/lumify

Dokumen atau media digital ini dan informasi yang terkandung di dalamnya merupakan informasi rahasia dan milik Philips serta tidak dapat dicetak ulang, disalin baik keseluruhan maupun sebagian, diadaptasi, dimodifikasi, diungkapkan kepada pihak lain, atau disebarluaskan tanpa izin tertulis sebelumnya dari Bagian Legal Philips. Dokumen atau media digital ini ditujukan untuk digunakan oleh pelanggan dan dilisensikan kepada pelanggan sebagai bagian dari pembelian peralatan Philips, atau untuk memenuhi kesesuaian peraturan sebagaimana disyaratkan oleh FDA dalam bagian 21 CFR 1020.30 (dan setiap amandemennya) dan persyaratan peraturan setempat lainnya. Orang yang tidak berwenang dilarang keras menggunakan dokumen atau media digital ini.

4535 619 63091_A/795 * FEB 2018

Philips

Philips memberikan dokumen ini tanpa garansi apa pun, baik tersirat maupun tersurat, termasuk namun tidak terbatas pada garansi tersirat atas kelayakan untuk diperdagangkan, dan kesesuaian untuk tujuan tertentu.

Philips telah memastikan keakuratan dokumen ini. Namun demikian, Philips tidak bertanggung jawab atas kesalahan atau kekurangan apa pun dan berhak untuk membuat perubahan tanpa pemberitahuan lebih lanjut pada setiap produk yang disebutkan dalam dokumen ini untuk meningkatkan keandalan, fungsi, atau desain. Philips dapat melakukan penyempurnaan atau perubahan pada produk atau program yang dijelaskan dalam dokumen ini setiap saat.

Philips tidak memberikan pernyataan atau jaminan apa pun kepada pengguna atau pihak lain berkenaan dengan kelengkapan dokumen ini untuk tujuan tertentu atau berkenaan dengan kelengkapannya untuk memperoleh hasil tertentu. Hak pengguna atas pemulihan terhadap kerusakan yang disebabkan oleh kesalahan atau kelalaian pada komponen Philips terbatas pada jumlah yang dibayarkan oleh pengguna kepada Philips berdasarkan ketentuan dokumen ini. Dalam hal apa pun Philips tidak bertanggung jawab atas kerusakan, kerugian, ongkos, biaya, klaim, tuntutan, atau klaim atas hilangnya keuntungan, data, pembayaran, atau pengeluaran dalam bentuk atau jenis apa pun secara khusus, tambahan, kebetulan baik langsung maupun tidak langsung atau sebab akibat.

Penyalinan dokumen ini tanpa izin tertulis, selain melanggar hak cipta, dapat mengurangi kemampuan Philips untuk memberikan informasi yang akurat dan aktual kepada pengguna.

Nama produk yang bukan Philips mungkin merupakan merek dagang dari pemilik yang bersangkutan.

4535 619 63091_A/795 * FEB 2018

Informasi Umum

Informasi umum berikut ini berlaku untuk keamanan perangkat lunak ultrasound Philips dan data pasien.

- Sistem ultrasound Philips tidak mendukung pengoperasian sesi-lebih-dari-satu-pengguna. Sistem ini dirancang sebagai perangkat untuk satu pengguna. Akses penggunaan klinis melalui jaringan tidak didukung.
- Sistem ultrasound bukan perangkat penyimpanan jangka panjang. Data pasien tetap harus diarsipkan ke DICOM PACS, jaringan bersama, atau direktori lokal.

2 Kontrol terhadap Kerentanan Keamanan pada Produk Philips

Philips berkomitmen untuk membantu semua pelanggan dalam hal menjaga kerahasiaan, integritas, dan ketersediaan data pasien sekaligus memastikan bahwa sistem ultrasound pelanggan dapat terus menghasilkan dan mengelola informasi ini dengan keamanan lengkap. Sistem ultrasound dapat menjadi rentan terhadap pelanggaran keamanan bila tersambung ke jaringan.

Strategi Keamanan dengan Pertahanan Berlapis

Di dalam organisasi perawatan kesehatan, pemeliharaan keamanan data pasien dan produk Philips memerlukan strategi keamanan bertingkat yang menyeluruh dan berlapis (termasuk kebijakan, proses, dan teknologi) untuk melindungi informasi dan sistem dari ancaman internal dan eksternal.

Untuk informasi khusus mengenai keamanan di dalam organisasi Anda, hubungi spesialis keamanan di kantor berikut atau kantor yang menjalankan tanggung jawab serupa:

- Chief information security officer (CISO)
- Chief Information Officer
- HIPAA Privacy atau Security Officer (di Amerika Serikat)
- Safety officer

Untuk mengetahui tentang masalah keamanan umum atau kerentanan khusus pada sistem ultrasound Anda, hubungi perwakilan Philips Anda.

4535 619 63091_A/795 * FEB 2018

Philips

Lingkungan Pengaturan

Pengembangan dan produksi perangkat medis diatur secara ketat sebagaimana keamanan dan kerahasiaan informasi pasien yang disimpan oleh penyedia perawatan kesehatan. Hal ini menciptakan tantangan bagi penyedia perawatan kesehatan dan produsen dalam merespons dengan cepat indikasi ancaman terhadap keamanan data pasien yang tersimpan di perangkat medis.

Perlindungan Terhadap Informasi Elektronik Kesehatan Pasien

Informasi kesehatan pasien merupakan salah satu aset paling penting yang harus dilindungi dengan tindakan keamanan. Contoh, peraturan berikut menyatakan bahwa informasi kesehatan pasien harus dijaga kerahasiaannya, dan peraturan tersebut menjelaskan langkah-langkah keamanan untuk melindungi informasi pasien:

- HIPAA (Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan) Amerika Serikat (www.hhs.gov/ocr/privacy/)
- Petunjuk Perangkat Medis Eropa 93/42/EEC
- HPB517 Jepang
- Bagian mengenai HIPAA dari undang-undang pendorong ekonomi federal AS (atau HITECH), secara formal dikenal sebagai American Recovery and Reinvestment Act tahun 2009

Peran Philips dalam Kemitraan Keamanan Produk

Philips beroperasi berdasarkan Kebijakan Keamanan Produk global yang mengatur desain untuk keamanan dalam pembuatan produk, penilaian risiko, dan aktivitas tanggap insiden terhadap kerentanan yang teridentifikasi pada produk yang ada. Philips telah menerapkan pelacakan masalah global dan proses eskalasi yang memberikan visibilitas untuk masalah keamanan yang melibatkan sistem Philips.

4535 619 63091_A/795 * FEB 2018

Philips

Respons Terhadap Kerentanan

Grup teknik produk di Philips terus-menerus memantau kerentanan keamanan baru di sistem kami, termasuk yang teridentifikasi oleh perangkat lunak pihak ketiga dan vendor sistem operasi dan yang dilaporkan dari organisasi perawatan kesehatan individu.

Jaringan global untuk tim bantuan yang dikhususkan untuk menangani insiden terkait keamanan produk mengumpulkan dan mengelola kerentanan yang memengaruhi produk dan solusi Philips. Tim bantuan terus meluaskan aktivitas mereka terhadap cakupan global seluruh sistem.

Tujuannya adalah agar tim bantuan terkait dapat mengevaluasi setiap pelanggaran keamanan yang nyata dan potensial dengan penilaian yang jelas terhadap risiko, ancaman, atau kerentanan, dan untuk mengembangkan, sebagaimana diperlukan, rencana bantuan kerentanan yang mencakup prosedur kualifikasi dan komunikasi. Artinya, Philips bertujuan untuk secara serentak menginformasikan kepada pelanggan tentang kerentanan sistem sekaligus melanjutkan pengembangan dan pengerahan upaya pengurangan risiko. Untuk informasi lebih lanjut tentang kerentanan sistem, lihat situs web ini:

www.philips.com/productsecurity

Penyempurnaan Desain

Philips secara aktif melakukan penilaian keamanan produk internal untuk mengidentifikasi kemungkinan kelemahan keamanan. Dengan informasi tersebut, tim teknik Philips secara teratur menetapkan perubahan konfigurasi dan merekayasa balik upaya-upaya yang memperkuat sistem terhadap ancaman luar. Informasi yang sama juga mendorong persyaratan desain keamanan untuk produk baru. Kebijakan Keamanan Produk Philips mensyaratkan tujuan desain untuk keamanan sebagai bagian dari upaya pembuatan semua produk baru.

4535 619 63091_A/795 * FEB 2018

Philips

Peran Pelanggan dalam Kemitraan Keamanan Produk

PERINGATAN

Modifikasi tanpa izin ke perangkat Android Anda ("rooting" atau "jailbreaking") dapat menyebabkan gangguan fungsi sistem ultrasound sehingga mengakibatkan kesalahan diagnosis.

PERHATIAN

Perangkat Android memiliki banyak aplikasi yang tersedia untuk diinstal melalui Google Play store. Namun, untuk meminimalkan risiko terhadap keamanan data pasien, Philips menyarankan Anda untuk menginstal aplikasi hanya dari sumber tepercaya dan membatasi penggunaannya untuk kebutuhan bisnis.

Anda bertanggung jawab untuk memastikan keamanan perangkat Anda dan data pasien agar dapat memenuhi kebijakan keamanan dan persyaratan peraturan setempat. Hubungi departemen Keamanan TI Perawatan Kesehatan Anda untuk memastikan profil keamanan perangkat Anda dikonfigurasikan sesuai dengan persyaratan khusus untuk keamanan informasi.

Implementasi praktis dari elemen keamanan teknis berbeda-beda menurut lokasi dan dapat menggunakan sejumlah teknologi termasuk firewall, perangkat lunak pemindaian virus, teknologi autentikasi, dan seterusnya. Seperti halnya setiap sistem berbasis komputer, sistem ultrasound memerlukan tingkat perlindungan yang secara umum diberikan oleh firewall dan perangkat keamanan lain antara sistem medis dan sistem yang dapat diakses secara eksternal. Department of Veterans Affairs AS telah mengembangkan arsitektur isolasi yang secara luas digunakan untuk tujuan ini. Pertahanan perimeter dan jaringan tersebut merupakan elemen mendasar dari praktik keamanan yang baik. *Panduan Arsitektur Isolasi Perangkat Medis* Department of Veterans Affairs terdapat di situs web ini:

http://www.himss.org/ResourceLibrary/ResourceDetail.aspx?ItemNumber=7236

4535 619 63091_A/795 * FEB 2018

Philips

Respons terhadap Insiden Keamanan Produk dan Deteksi Malware

Jika terjadi insiden terkait keamanan produk, atau jika Anda mendeteksi malware (perangkat lunak berbahaya) pada sistem, segera putuskan sambungan sistem dari jaringan dan laporkan insiden tersebut ke bagian Keamanan TI Perawatan Kesehatan Anda. Selain itu, laporkan insiden dengan mengirim e-mail ke:

productsecurity@philips.com

Masalah Keamanan dan Panduan Keamanan

Panduan berikut memberikan contoh nyata kerentanan sistem dan data serta metode untuk memberikan perlindungan.

CATATAN

Alat untuk manajemen perangkat seluler yang terpusat tersedia untuk memfasilitasi panduan dalam dokumen ini dan untuk memudahkan penerapan, konfigurasi, dan masalah keamanan. Hubungi bagian keamanan TI perawatan kesehatan organisasi Anda.

Persyaratan Perangkat

Philips menyarankan untuk memulai dengan konfigurasi perangkat yang memenuhi atau melebihi persyaratan minimum aplikasi Lumify, serta kebutuhan keamanan di lingkungan Anda. Langkah berikutnya adalah memastikan bahwa level kontrol keamanan yang layak telah diterapkan dengan cara yang sesuai dengan kebijakan keamanan setempat Anda serta kewajiban peraturan yang berlaku.

Pelindungan Perangkat

Serupa dengan prinsip strategi pelindungan OS yang digunakan di desktop atau laptop, pelindungan perangkat meliputi identifikasi semua fungsi dan aplikasi yang tidak diperlukan di perangkat Anda dan menonaktifkan fungsi tersebut atau aplikasi yang tidak perlu digunakan.

4535 619 63091_A/795 * FEB 2018

Philips

Tergantung pada perangkatnya, hal ini juga dapat meliputi penonaktifan kemampuan aplikasi untuk menjalankan fungsionalitas latar belakang yang memengaruhi kinerja perangkat Anda saat Lumify digunakan. Pelindungan perangkat akan mengurangi titik serang pada perangkat Anda dengan menghilangkan layanan yang dapat menjadi rentan seiring waktu.

Enkripsi

Kontrol keamanan utama yang tersedia di hampir semua perangkat Android adalah enkripsi. Enkripsi memastikan data yang tersimpan pada sistem terlindungi dan meningkatkan kekuatan kebijakan kontrol akses Anda dengan merender data yang tidak dapat dipulihkan.

Keamanan Jaringan

Setiap sistem ultrasound dalam jaringan harus tersambung ke jaringan lokal yang aman, yang memberikan perlindungan terhadap virus komputer dan kode jahat atau lalu lintas berbahaya lainnya. Pastikan jaringan area lokal (LAN) menggunakan perlindungan yang sesuai, misalnya hanya menggunakan teknologi nirkabel yang aman, firewall, sistem pendeteksian dan pencegahan intrusi, serta pemindai kerentanan.

Kontrol Akses Fisik

Setiap organisasi perawatan kesehatan harus membatasi akses fisik ke sistem ultrasound untuk mencegah kontak secara kebetulan, sambil lalu, ataupun disengaja oleh individu yang tidak berwenang. Kantor keselamatan atau keamanan organisasi dapat memberikan informasi lebih lanjut tentang tindakan yang berlaku.

Posisi Perangkat

Akses untuk melihat informasi yang dilindungi tanpa izin dapat diminimalkan dengan memosisikan perangkat agar tidak terlihat dari pintu, lorong, dan area lalu-lalang lainnya. Aktifkan layar kosong dengan log off dari sistem atau kosongkan tampilan layar secara manual sebelum Anda meninggalkan perangkat tanpa pengawasan untuk sementara waktu.

4535 619 63091_A/795 * FEB 2018

Philips

Perlindungan Login dan Logout Pengguna

Dengan sendirinya, kata sandi melindungi penyimpanan informasi kesehatan yang dilindungi (PHI, protected health information) dari akses tanpa izin, di samping memenuhi syarat keamanan untuk pengoperasian perangkat yang sesegera mungkin.

Memperhatikan ukuran dan portabilitas perangkat tablet dan menerapkan kata sandi atau kode sandi sangat penting untuk mengurangi potensi pengungkapan informasi pribadi jika sistem salah tempat atau dicuri. Pada beberapa perangkat, kontrol tambahan mungkin diterapkan untuk menghapus semua data dari perangkat jika kata sandi atau kode sandi salah dimasukkan beberapa kali. Kontrol tersebut membantu meningkatkan model kontrol akses standar dan mengurangi potensi pengungkapan informasi pribadi.

Untuk perangkat dengan fungsi login, proses login pengguna yang konsisten, termasuk nama pengguna dan kata sandi, akan memberikan keamanan yang baik dalam melindungi informasi. Organisasi perawatan kesehatan harus senantiasa mengontrol akses ke sistem.

Praktik login dan kata sandi yang dilindungi mencakup hal berikut:

- Menerapkan kata sandi yang kuat. Ini merupakan metode yang paling mudah dan efektif untuk meningkatkan keamanan. Kata sandi yang kuat berisi minimal delapan karakter alfanumerik, campuran huruf besar dan huruf kecil, serta karakter khusus seperti “@” atau “*”. Jangan gunakan kata-kata yang dapat ditemukan dalam kamus.
- Jangan mengirim atau membagikan nama pengguna dan kata sandi.
- Ubah kata sandi secara berkala.

Latih operator sistem untuk log off dari sistem secepatnya setelah menyelesaikan pekerjaan.

Contoh Pemeliharaan Informasi

Contoh ini menunjukkan cara memelihara keamanan informasi menggunakan model zona aliran informasi.

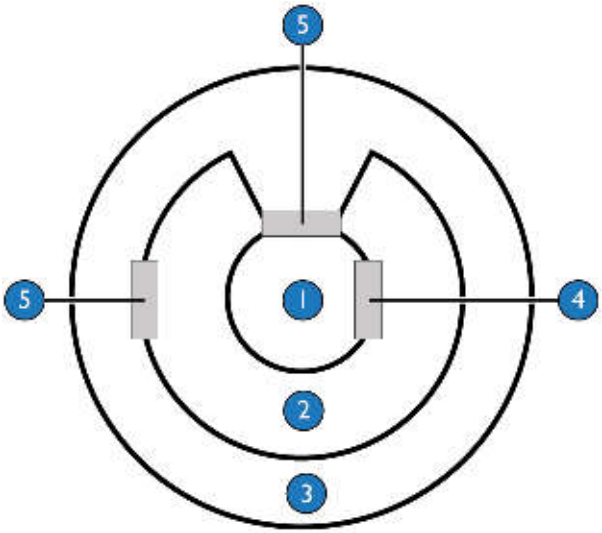
4535 619 63091_A/795 * FEB 2018

Asumsi Tentang Lingkungan

Sistem ultrasound harus didukung oleh organisasi perawatan kesehatan untuk menjaga lingkungan yang aman, dengan mekanisme perlindungan untuk akses jaringan, enkripsi, dan deteksi penyusupan.

Zona Informasi

Model aliran informasi biasanya diintegrasikan dengan standar keamanan. Cara mudah untuk memvisualisasikan model ini adalah dengan membuat diagram organisasi perawatan kesehatan yang dibagi dalam tiga zona (lihat gambar), dengan tiap-tiap zona memiliki prioritas dan tingkat pemanfaatan atas informasi yang berbeda. Beberapa organisasi memutuskan untuk tidak menyebarkan informasi mereka ke zona yang lebih jauh karena mereka tidak dapat menjamin perlindungan dan integritasnya.



Solusi Keamanan Antar Zona

1	Zona 1: Divisi ultrasound
2	Zona 2: Divisi lain di organisasi perawatan kesehatan

4535 619 63091_A/795 * FEB 2018

3	Zona 3: Internet
4	Firewall
5	Firewall dengan IPSec

Zona 1: Divisi Ultrasound

Sebagian besar pemindahan citra dilakukan dalam Zona 1. Cadangan, salinan, dan media yang berisi citra ultrasound harus dikelola dengan hati-hati oleh staf divisi terkait.

Zona 2: Divisi Lain di Organisasi Perawatan Kesehatan

Zona 2 mencakup fasilitas kesehatan di luar divisi yang memiliki akses ke sistem, dan dalam beberapa kasus, memiliki akses Internet. Autorisasi yang diperlukan untuk mengakses dan menggunakan jejak audit sangat penting.

Zona 3: Internet

Zona 3 digunakan untuk konektivitas ke penyedia penyimpanan cloud yang sesuai dengan HIPAA.

Keamanan Antar Zona

Keamanan antar zona harus dikelola berdasarkan solusi keamanan TI standar. Pengelola harus peka terhadap tingkat lalu lintas data yang diharapkan untuk memilih solusi yang aman, sekaligus menghindari kepadatan di titik tertentu dalam aliran informasi. Distribusi citra memerlukan jaringan dengan bandwidth tinggi.

Keamanan Dalam Zona

Keamanan di setiap zona harus dikelola berdasarkan gabungan dari solusi keamanan TI standar dan fungsi keamanan dari sistem ultrasound.

4535 619 63091_A/795 * FEB 2018

Perangkat Lunak Perlindungan Keamanan

Pembaruan aplikasi Lumify tersedia melalui rilis berkala dan proses Usulan Perubahan Bidang Philips.

Pemindaian dan Pembaruan Antivirus

Penerapan kebijakan keamanan jaringan yang efektif oleh organisasi perawatan kesehatan merupakan perlindungan terbaik terhadap virus.

Malware adalah penyebab utama banyak pelanggaran yang menjadi berita utama saat ini. Metode tradisional perlindungan malware meliputi Anti-Virus (AV). Philips menyarankan untuk memilih paket perangkat lunak terkemuka yang dapat memenuhi kebutuhan perlindungan terhadap malware. Langkah tambahan dapat diambil untuk membatasi potensi malware pada sistem Anda. Langkah tersebut juga memastikan apakah aplikasi tambahan yang ditambahkan ke perangkat Anda berasal dari sumber terkemuka. Karena aplikasi mungkin menyertakan malware, cukup instal aplikasi yang diperlukan untuk fungsionalitas perangkat guna membatasi risiko terkena virus atau pelanggaran.

Cadangan dan Arsip

PERHATIAN

Tujuan dan mekanisme ekspor yang dipilih harus sesuai dengan kebijakan keamanan TI perawatan kesehatan setempat Anda.

Anda dapat mengekspor pemeriksaan dan citra dari sistem ultrasound Lumify ke DICOM PACS, jaringan bersama, atau direktori lokal. Anda juga dapat mengirimkan citra melalui email.

4535 619 63091_A/795 * FEB 2018

Philips

Prosedur Pencadangan

Sistem ultrasound dirancang untuk menyimpan informasi yang diperlukan dalam pembuatan dokumen eksternal bagi rekam medis saja (seperti film, jejak, dan rekam cetak). Jika cadangan tambahan diperlukan, tetapkan protokol administratif untuk mengarsipkan semua pengamatan klinis sebelum penghapusan dilakukan.

Rencana Pemulihan Kerusakan

Anda bertanggung jawab sepenuhnya untuk menyiapkan rencana pemulihan kerusakan yang mencakup pencadangan secara berkala dan pencadangan lengkap data pasien. Sistem ultrasound bukan perangkat penyimpanan jangka panjang sehingga data pasien harus diekspor dari sistem ultrasound. Untuk informasi lebih lanjut tentang mengekspor data pasien, lihat informasi pengguna sistem ultrasound Anda.

4535 619 63091_A/795 * FEB 2018

Philips

www.philips.com/healthcare

Philips Ultrasound, Inc.
22100 Bothell Everett Hwy
Bothell, WA 98021-8431
USA

EC REP

Philips Medical Systems Nederland B.V.
Veenpluis 4-6
5684 PC Best
The Netherlands

CE 0086

© 2018 Koninklijke Philips N.V.
Semua hak dilindungi undang-undang. Memperbanyak atau mengirimkan secara keseluruhan atau sebagian dalam bentuk apa pun atau dengan cara apa pun, elektronik, mekanis, atau selain itu dilarang tanpa izin tertulis sebelumnya dari pemilik hak cipta.

Diterbitkan di Amerika Serikat
4535 619 63091_A/795 * FEB 2018 - id-ID