CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

21 Juni 2022

EDISI 109

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	3
URGENT	0	0	0
IMPORTANT	2	1	0

General News

Twitter Akan Mendorong Pengguna untuk Meninjau Balasan dengan Bahasa yang Berbahaya atau Menyinggung

Twitter mengambil langkah proaktif untuk membatasi penyalahgunaan media sosial. Saat ini, menurut Mukul Sharma, Twitter sedang menguji fitur baru yang akan mendorong pengguna untuk meninjau balasan dengan bahasa yang berpotensi berbahaya atau menyinggung. Twitter akan memberikan tombol edit untuk menghapus kata-kata yang berpotensi melukai perasaan atau mengintimidasi. Pencegahan dilakukan dengan menampilkan peringatan yang menyatakan bahwa *tweet* dengan bahasa kasar tertentu dapat saja membuat pengguna dipenjara. Selain itu, Twitter juga menghadirkan fitur *downvote* untuk membantu Twitter memahami jenis konten yang ingin dilihat pengguna.

Prioritas: *3. Important*

< https://www.neowin.net/news/twitter-will-encourage-users-to-review-replies-with-harmful-or-offensive-language/>

QNAP Kembali Ditargetkan dalam Serangan Baru yang Melibatkan DeadBolt dan eCh0raix

Perangkat QNAP NAS kembali menjadi sasaran dalam kampanye serangan baru yang melibatkan *ransomware* DeadBolt dan eCh0raix. Sebelumnya, pada Januari 2022, penyerang menuntut penebusan sejumlah 0,03 BTC sebagai ganti kunci dekripsi, 5 BTC sebagai imbalan atas informasi *zero-day* di perangkat QNAP NAS, dan 50 BTC untuk kunci master dekripsi dan detail lengkap tentang kerentanan. Pekan lalu, QNAP menerbitkan sebuah imbauan keamanan untuk memperingatkan kampanye *ransomware* DeadBolt baru yang menargetkan perangkat NAS yang menjalankan versi QTS 4.x. Saat ini, serangan tersebut masih dalam tahap investigasi oleh pihak QNAP, namun perusahaan mendesak pengguna untuk memperbarui QTS hero atau QuTS ke versi terbaru yang tersedia.

Prioritas: ***3. Important***

< https://www.securityweek.com/qnap-appliances-targeted-new-deadbolt-ech0raix-ransomware-campaigns >

Breachs/Hacks/Leaks

Pelanggaran Data 1,5 Juta Pelanggan pada Flagstar Bank

Flagstar memberitahukan pelanggaran data yang dikirim ke pelanggan terpapar bahwa terdapat 1,5 juta pelanggan yang terkena pelanggaran data. Peretas mengakses data pribadi milik pelanggan sepanjang Desember 2021. Hasil penyelidikan pada 2 Juni 2022 menyebutkan bahwa peretas mengakses detail pelanggan yang sensitif, termasuk nama lengkap dan nomor jaminan sosial. Sampel data yang dicuri termasuk nama, SSN, alamat, catatan pajak, dan nomor telepon, dan akhirnya dipublikasikan di situs Clop. Insiden ini memengaruhi banyak entitas yang berbisnis dengan Accellion, Bombardier, Singtel, New Zealand Reserve Bank, dan Washington's State Auditor.

Prioritas: ***3. Important***

< https://www.bleepingcomputer.com/news/security/flagstar-bank-discloses-data-breach-impacting-15-million-customers/ >

Vulnerabilities

Serangan DFSCoerce NTLM *Relay* Memungkinkan Pengambilalihan Domain Windows

Layanan infrastruktur kunci publik di domain Windoes, Microsoft Active Directory Certificate Services, rentan terhadap serangan NTLM *Relay,* yaitu ketika pelaku ancaman memaksa pengontrol domain untuk mengautentikasi *relay* berbahaya di bawah kendali penyerang. Hal ini memungkinkan pelaku ancaman untuk memperoleh hak istimewa yang lebih tinggi atau bahkan pengambilalihan domain dan menjalankan perintah apapun. Pemaksaan dapat dilakukan menggunakan berbagai metode, termasuk protokol MS-RPRN, MS-EFSRPC (PetitPotam), dan MS-FSRVP. Minggu ini, peneliti keamanan Filip Dragovic merilis skrip *proof-of-concept* untuk serangan NTLM *Relay* yang disebut sebagai "DFSCoerce" menggunakan protokol MS-DFSNM untuk menyampaikan autentikasi terhadap server arbitrer.

Prioritas: ***1. Critical***

< https://www.bleepingcomputer.com/news/microsoft/new-dfscoerce-ntlm-relay-attack-allows-windows-domain-takeover/ >

Peneliti Google Merinci Kerentanan Apple Safari yang Dieksploitasi

Kerentanan keamanan pada Apple Safari yang dieksploitasi di awal tahun 2022 awalnya diperbaiki pada 2013 dan diperkenalkan kembali pada Desember 2016. Kerentanan ini terus ada selama lima tahun hingga ditetapkan sebagai *zero-day* pada Januaru 2022. Kerentanan yang dilacak sebagai CVE-2022-22620 dengan skor CVSS 8,8 ini menyangkut kasus kerentanan *use-after-free* dalam komponen WebKit yang dapat diekspolitasi oleh sepotong konten web yang dibuat khusus untuk mendapatkan eksekusi kode arbitrer. Meskipun kerentanan pada tahun 2013 dan 2022 ini pada dasarnya sama, jalur untuk memicu kerentanan berbeda. Maddie Stone menekankan pengauditan kode dan tambalan untuk menghindari contoh duplikasi perbaikan dan memahami dampak keamanan dari perubahan yang dilakukan.

Prioritas: ***1. Critical***

< https://thehackernews.com/2022/06/google-researchers-detail-5-year-old.html?&web_view=true >

Pembaruan Darurat Windows Perbaiki Masalah Microsoft 365 pada Perangkat Arm

Microsoft telah merilis pembaruan Windows *out-of-bound* (OOB) untuk mengatasi masalah umum yang akan menyebabkan masalah *login* Azure Active Directory dan Microsoft 365 pada perangkat Arm. Pembaruan OOB ini akan diinstal secara otomatis melalui Windows Update dan dapat diunduh secara manual melalui Microsoft Update Catalog (KB5016139 untuk Windows 10 dan KB5016138 untuk Windows 11). Vresi Windows yang terpengaruh masalah ini mencakup Windows 11 21H2, Windows 10 21H2, Windows 10 21H1, dan Windows 10 20H2. Pembaruan ini juga menimbulkan beberapa masalah lain, seperti gangguan konektivitas *hotspot* Wi-Fi, masalah koneksi VPN dan RDP di server dengan RRAS diaktifkan.

Prioritas: ***1. Critical***

< https://www.bleepingcomputer.com/news/microsoft/windows-emergency-update-fixes-microsoft-365-issues-on-arm-devices/ >