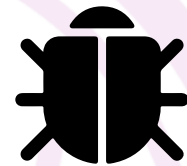


# SECURITY ADVISORY

## CVE-2024-21413



CVE-2024-21413 adalah kerentanan eksekusi kode jarak jauh yang ditemukan di Microsoft Outlook. Kerentanan ini memungkinkan penyerang untuk mengeksekusi kode berbahaya di sistem target dengan memanfaatkan validasi input yang tidak memadai. Dengan memanfaatkan kelemahan ini, penyerang dapat mengambil alih kendali sistem yang terinfeksi, menyebabkan kerusakan data dan potensi pengambilalihan sistem.

Nilai/Tingkat

# 9.8

Critical

### CWE **20** Improper Input Validation

CWE-20 merujuk pada kesalahan dalam memvalidasi input yang masuk ke dalam sistem, yang memungkinkan penyerang untuk mengirimkan data berbahaya yang dapat dieksekusi di sistem target. Validasi input yang tidak memadai memungkinkan serangan yang dapat mengganggu integritas dan keamanan sistem.

### Langkah Mitigasi

Untuk mengurangi risiko dan melindungi sistem dari eksploitasi kerentanan ini, disarankan untuk segera melakukan pembaruan perangkat lunak Microsoft Outlook dan produk terkait ke versi terbaru yang telah diperbaiki. Pembaruan ini tersedia melalui Office Security Releases.

### Produk Terancam

- Microsoft Office 2019 19.0.0 dan sebelumnya
- Microsoft 365 Apps for Enterprise 16.0.1 dan sebelumnya
- Microsoft Office LTSC 2021 16.0.1 dan sebelumnya
- Microsoft Office 2016 16.0.5435.1001

### Referensi Lanjutan, Solusi, dan Alat

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21413>
- <https://learn.microsoft.com/en-us/officeupdates/microsoft365-apps-security-updates>
- <https://blog.injectexp.dev/outlook-cve-2024-21413-for-rce-hacking-through-a-letter/07/rce/>



Informasi  
Imbauan Keamanan  
Lainnya di laman  
**Id-SIRTII/CC**

<https://www.idsirtii.or.id/peringatan.html>

### Sumber Penulisan

- [Diakses 31 Juli 2024] <https://www.cve.org/CVERecord?id=CVE-2024-21413>
- [Diakses 31 Juli 2024] <https://nvd.nist.gov/vuln/detail/CVE-2024-21413>

TLP Level Clear ○○○

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

Diterbitkan Oleh

## Id-SIRTII/CC

Indonesia Security Incident  
Response team on Internet  
Infrastructure Coordination Center

Badan Siber dan Sandi Negara

(021) 788 33610

[bantuan70@bssn.go.id](mailto:bantuan70@bssn.go.id)

Jl. Harsono RM No. 70, Ragunan,  
Pasar Minggu, Jakarta Selatan 12550

