Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0010

## Kwetsbaarheden verholpen in Microsoft Windows

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-01-2025

**TLP:WHITE**

**Toegestane verspreiding van TLP:WHITE**
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

## Feiten

Microsoft heeft kwetsbaarheden verholpen in Windows.

## Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial of Service (DoS)
- Omzeilen van beveiligingsmaatregel
- Uitvoer van willekeurige code (Gebruikersrechten)
- Uitvoer van willekeurige code (Systeemrechten)
- Toegang tot gevoelige gegevens
- Verkrijgen van verhoogde rechten
- Spoofing

Van de kwetsbaarheid met kenmerk CVE-2025-21308 geeft Microsoft aan informatie te hebben dat de kwetsbaarheid besproken wordt op gesloten fora. Deze kwetsbaarheid bevindt zich in het Thema-systeem en stelt een kwaadwillende in staat om zich voor te doen als het slachtoffer en mogelijk code uit te voeren in de context van het slachtoffer. Succesvol misbruik is niet eenvoudig en vereist dat de kwaadwillende het slachtoffer misleidt een malafide bestand te openen en bewerken. Grootschalig actief misbruik is daarmee onwaarschijnlijk.

```
Windows Security Account Manager:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-21313 | 6.50 | Denial-of-Service                   |
|----------------|------|-------------------------------------|

Windows Web Threat Defense User Service:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
| CVE-2025-21343 | 7.50 | Toegang tot gevoelige gegevens      |
|----------------|------|-------------------------------------|

Windows Smart Card:
|----------------|------|-------------------------------------|
| CVE-ID         | CVSS | Impact                              |
|----------------|------|-------------------------------------|
```

| CVE-2025-21312 | 2.40 | Toegang tot gevoelige gegevens |

Microsoft Windows Search Component:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21292 | 8.80 | Verkrijgen van verhoogde rechten |

Windows WLAN Auto Config Service:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21257 | 5.50 | Toegang tot gevoelige gegevens |

Windows Remote Desktop Services:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21297 | 8.10 | Uitvoeren van willekeurige code |
| CVE-2025-21309 | 8.10 | Uitvoeren van willekeurige code |
| CVE-2025-21278 | 6.20 | Denial-of-Service |
| CVE-2025-21330 | 7.50 | Denial-of-Service |
| CVE-2025-21225 | 5.90 | Denial-of-Service |

Windows Virtual Trusted Platform Module:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21210 | 4.20 | Toegang tot gevoelige gegevens |
| CVE-2025-21280 | 5.50 | Denial-of-Service |
| CVE-2025-21284 | 5.50 | Denial-of-Service |

Windows Kernel Memory:

| CVE-ID | CVSS | Impact |
|---|---|---|

| CVE-2025-21316 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21318 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21319 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21320 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21321 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21317 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21323 | 5.50 | Toegang tot gevoelige gegevens |

Windows NTLM:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21311 | 9.80 | Verkrijgen van verhoogde rechten |

Windows Recovery Environment Agent:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21202 | 6.10 | Verkrijgen van verhoogde rechten |

Windows Themes:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21308 | 6.50 | Voordoen als andere gebruiker |

Windows Secure Boot:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2024-7344 | 6.70 | Omzeilen van beveiligingsmaatregel |

Windows Geolocation Service:

| CVE-ID | CVSS | Impact |
|---|---|---|

| CVE-2025-21301 | 6.50 | Toegang tot gevoelige gegevens |

Windows Virtualization-Based Security (VBS) Enclave:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21370 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Boot Loader:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21211 | 6.80 | Omzeilen van beveiligingsmaatregel |

Windows UPnP Device Host:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21389 | 7.50 | Denial-of-Service |
| CVE-2025-21300 | 7.50 | Denial-of-Service |

Microsoft Brokering File System:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21315 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-21372 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Mark of the Web (MOTW):

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21217 | 6.50 | Voordoen als andere gebruiker |

Windows Connected Devices Platform Service:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21207 | 7.50 | Denial-of-Service |

Active Directory Federation Services:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21193 | 6.50 | Voordoen als andere gebruiker |

Microsoft Graphics Component:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21382 | 7.80 | Verkrijgen van verhoogde rechten |

Windows OLE:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21298 | 9.80 | Uitvoeren van willekeurige code |

Windows SmartScreen:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21314 | 6.50 | Voordoen als andere gebruiker |

Line Printer Daemon Service (LPD):

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21224 | 8.10 | Uitvoeren van willekeurige code |

Windows Direct Show:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21291 | 8.80 | Uitvoeren van willekeurige code |

Windows Kerberos:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21242 | 5.90 | Toegang tot gevoelige gegevens |
| CVE-2025-21299 | 7.10 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-21218 | 7.50 | Denial-of-Service |

Windows Installer:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21275 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-21287 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-21331 | 7.30 | Verkrijgen van verhoogde rechten |

Windows Cryptographic Services:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21336 | 5.60 | Toegang tot gevoelige gegevens |

Windows Win32K - GRFX:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21338 | 7.80 | Uitvoeren van willekeurige code |

Windows Digital Media:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21249 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21255 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21258 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21260 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21263 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21265 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21327 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21341 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21226 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21227 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21228 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21229 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21232 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21256 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21261 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21310 | 6.60 | Verkrijgen van verhoogde rechten |
| CVE-2025-21324 | 6.60 | Verkrijgen van verhoogde rechten |

Windows PrintWorkflowUserSvc:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21234 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-21235 | 7.80 | Verkrijgen van verhoogde rechten |

Windows MapUrlToZone:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21268 | 4.30 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-21269 | 4.30 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-21219 | 4.30 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-21329 | 4.30 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-21328 | 4.30 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-21189 | 4.30 | Omzeilen van beveiligingsmaatregel |
| CVE-2025-21276 | 7.50 | Denial-of-Service |
| CVE-2025-21332 | 4.30 | Omzeilen van beveiligingsmaatregel |

|----------------|------|-------------------------------------|

Active Directory Domain Services:

|----------------|------|-------------------------------------|
| CVE-ID | CVSS | Impact |
|----------------|------|-------------------------------------|
| CVE-2025-21293 | 8.80 | Verkrijgen van verhoogde rechten |
|----------------|------|-------------------------------------|

Windows COM:

|----------------|------|-------------------------------------|
| CVE-ID | CVSS | Impact |
|----------------|------|-------------------------------------|
| CVE-2025-21272 | 6.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21281 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-21288 | 6.50 | Toegang tot gevoelige gegevens |
|----------------|------|-------------------------------------|

Windows Event Tracing:

|----------------|------|-------------------------------------|
| CVE-ID | CVSS | Impact |
|----------------|------|-------------------------------------|
| CVE-2025-21274 | 5.50 | Denial-of-Service |
|----------------|------|-------------------------------------|

Windows Hyper-V NT Kernel Integration VSP:

|----------------|------|-------------------------------------|
| CVE-ID | CVSS | Impact |
|----------------|------|-------------------------------------|
| CVE-2025-21335 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-21333 | 7.80 | Verkrijgen van verhoogde rechten |
| CVE-2025-21334 | 7.80 | Verkrijgen van verhoogde rechten |
|----------------|------|-------------------------------------|

Windows Client-Side Caching (CSC) Service:

|----------------|------|-------------------------------------|
| CVE-ID | CVSS | Impact |
|----------------|------|-------------------------------------|
| CVE-2025-21374 | 5.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21378 | 7.80 | Verkrijgen van verhoogde rechten |
|----------------|------|-------------------------------------|

Windows SPNEGO Extended Negotiation:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21295 | 8.10 | Uitvoeren van willekeurige code |

Windows Cloud Files Mini Filter Driver:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21271 | 7.80 | Verkrijgen van verhoogde rechten |

IP Helper:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21231 | 7.50 | Denial-of-Service |

Reliable Multicast Transport Driver (RMCAST):

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21307 | 9.80 | Uitvoeren van willekeurige code |

Microsoft Digest Authentication:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21294 | 8.10 | Uitvoeren van willekeurige code |

Windows BitLocker:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21214 | 4.20 | Toegang tot gevoelige gegevens |

| CVE-2025-21213 | 4.60 | Omzeilen van beveiligingsmaatregel |
|---|---|---|

Internet Explorer:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21326 | 7.80 | Uitvoeren van willekeurige code |

Windows Telephony Service:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21411 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21413 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21233 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21236 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21237 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21239 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21241 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21243 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21244 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21248 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21252 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21266 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21282 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21302 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21303 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21306 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21273 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21286 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21305 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21339 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21246 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21417 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21250 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21240 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21238 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21223 | 8.80 | Uitvoeren van willekeurige code |
| CVE-2025-21409 | 8.80 | Uitvoeren van willekeurige code |

| CVE-2025-21245 | 8.80 | Uitvoeren van willekeurige code |

Windows Message Queuing:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21251 | 7.50 | Denial-of-Service |
| CVE-2025-21270 | 7.50 | Denial-of-Service |
| CVE-2025-21277 | 7.50 | Denial-of-Service |
| CVE-2025-21285 | 7.50 | Denial-of-Service |
| CVE-2025-21289 | 7.50 | Denial-of-Service |
| CVE-2025-21290 | 7.50 | Denial-of-Service |
| CVE-2025-21220 | 7.50 | Toegang tot gevoelige gegevens |
| CVE-2025-21230 | 7.50 | Denial-of-Service |

Windows DWM Core Library:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21304 | 7.80 | Verkrijgen van verhoogde rechten |

Windows Boot Manager:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21215 | 4.60 | Toegang tot gevoelige gegevens |

Windows Hello:

| CVE-ID | CVSS | Impact |
|---|---|---|
| CVE-2025-21340 | 5.50 | Omzeilen van beveiligingsmaatregel |

BranchCache:

| CVE-ID | CVSS | Impact |

```
|----------------|------|-------------------------------------|
| CVE-2025-21296 | 7.50 | Uitvoeren van willekeurige code     |
|----------------|------|-------------------------------------|
```

## Oplossingen

Microsoft heeft updates beschikbaar gesteld waarmee de beschreven kwetsbaarheden worden verholpen. We raden u aan om deze updates te installeren. Meer informatie over de kwetsbaarheden, de installatie van de updates en eventuele work-arounds vindt u op:

https://portal.msrc.microsoft.com/en-us/security-guidance

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2025-21411 | 8.8 HIGH |
| CVE-2025-21413 | 8.8 HIGH |
| CVE-2025-21210 | 4.2 MEDIUM |
| CVE-2025-21214 | 4.2 MEDIUM |
| CVE-2025-21215 | 4.6 MEDIUM |
| CVE-2025-21233 | 8.8 HIGH |
| CVE-2025-21236 | 8.8 HIGH |
| CVE-2025-21237 | 8.8 HIGH |
| CVE-2025-21239 | 8.8 HIGH |
| CVE-2025-21241 | 8.8 HIGH |
| CVE-2025-21242 | 5.9 MEDIUM |
| CVE-2025-21243 | 8.8 HIGH |
| CVE-2025-21244 | 8.8 HIGH |

| | |
|---|---|
| CVE-2025-21248 | 8.8 HIGH |
| CVE-2025-21249 | 6.6 MEDIUM |
| CVE-2025-21251 | 7.5 HIGH |
| CVE-2025-21252 | 8.8 HIGH |
| CVE-2025-21255 | 6.6 MEDIUM |
| CVE-2025-21257 | 5.5 MEDIUM |
| CVE-2025-21258 | 6.6 MEDIUM |
| CVE-2025-21260 | 6.6 MEDIUM |
| CVE-2025-21263 | 6.6 MEDIUM |
| CVE-2025-21265 | 6.6 MEDIUM |
| CVE-2025-21266 | 8.8 HIGH |
| CVE-2025-21268 | 4.3 MEDIUM |
| CVE-2025-21269 | 4.3 MEDIUM |
| CVE-2025-21270 | 7.5 HIGH |
| CVE-2025-21271 | 7.8 HIGH |
| CVE-2025-21272 | 6.5 MEDIUM |
| CVE-2025-21277 | 7.5 HIGH |
| CVE-2025-21280 | 5.5 MEDIUM |
| CVE-2025-21281 | 7.8 HIGH |
| CVE-2025-21282 | 8.8 HIGH |
| CVE-2025-21284 | 5.5 MEDIUM |
| CVE-2025-21285 | 7.5 HIGH |
| CVE-2025-21288 | 6.5 MEDIUM |

| | |
|---|---|
| CVE-2025-21289 | 7.5 HIGH |
| CVE-2025-21290 | 7.5 HIGH |
| CVE-2025-21291 | 8.8 HIGH |
| CVE-2025-21293 | 8.8 HIGH |
| CVE-2025-21294 | 8.1 HIGH |
| CVE-2025-21295 | 8.1 HIGH |
| CVE-2025-21296 | 7.5 HIGH |
| CVE-2025-21298 | 9.8 CRITICAL |
| CVE-2025-21299 | 7.1 HIGH |
| CVE-2025-21301 | 6.5 MEDIUM |
| CVE-2025-21302 | 8.8 HIGH |
| CVE-2025-21303 | 8.8 HIGH |
| CVE-2025-21304 | 7.8 HIGH |
| CVE-2025-21306 | 8.8 HIGH |
| CVE-2025-21314 | 6.5 MEDIUM |
| CVE-2025-21316 | 5.5 MEDIUM |
| CVE-2025-21318 | 5.5 MEDIUM |
| CVE-2025-21319 | 5.5 MEDIUM |
| CVE-2025-21320 | 5.5 MEDIUM |
| CVE-2025-21321 | 5.5 MEDIUM |
| CVE-2025-21327 | 6.6 MEDIUM |
| CVE-2025-21341 | 6.6 MEDIUM |
| CVE-2025-21382 | 7.8 HIGH |

| | |
|---|---|
| CVE-2025-21219 | 4.3 MEDIUM |
| CVE-2024-7344 | |
| CVE-2025-21389 | 7.5 HIGH |
| CVE-2025-21217 | 6.5 MEDIUM |
| CVE-2025-21278 | 6.2 MEDIUM |
| CVE-2025-21329 | 4.3 MEDIUM |
| CVE-2025-21328 | 4.3 MEDIUM |
| CVE-2025-21330 | 7.5 HIGH |
| CVE-2025-21220 | 7.5 HIGH |
| CVE-2025-21207 | 7.5 HIGH |
| CVE-2025-21202 | 6.1 MEDIUM |
| CVE-2025-21211 | 6.8 MEDIUM |
| CVE-2025-21213 | 4.6 MEDIUM |
| CVE-2025-21226 | 6.6 MEDIUM |
| CVE-2025-21227 | 6.6 MEDIUM |
| CVE-2025-21228 | 6.6 MEDIUM |
| CVE-2025-21229 | 6.6 MEDIUM |
| CVE-2025-21230 | 7.5 HIGH |
| CVE-2025-21231 | 7.5 HIGH |
| CVE-2025-21232 | 6.6 MEDIUM |
| CVE-2025-21256 | 6.6 MEDIUM |
| CVE-2025-21261 | 6.6 MEDIUM |
| CVE-2025-21189 | 4.3 MEDIUM |

| | |
|---|---|
| CVE-2025-21273 | 8.8 HIGH |
| CVE-2025-21274 | 5.5 MEDIUM |
| CVE-2025-21276 | 7.5 HIGH |
| CVE-2025-21286 | 8.8 HIGH |
| CVE-2025-21287 | 7.8 HIGH |
| CVE-2025-21292 | 8.8 HIGH |
| CVE-2025-21300 | 7.5 HIGH |
| CVE-2025-21305 | 8.8 HIGH |
| CVE-2025-21307 | 9.8 CRITICAL |
| CVE-2025-21308 | 6.5 MEDIUM |
| CVE-2025-21310 | 6.6 MEDIUM |
| CVE-2025-21312 | 2.4 LOW |
| CVE-2025-21323 | 5.5 MEDIUM |
| CVE-2025-21324 | 6.6 MEDIUM |
| CVE-2025-21331 | 7.3 HIGH |
| CVE-2025-21336 | 5.6 MEDIUM |
| CVE-2025-21338 | 7.8 HIGH |
| CVE-2025-21339 | 8.8 HIGH |
| CVE-2025-21340 | 5.5 MEDIUM |
| CVE-2025-21374 | 5.5 MEDIUM |
| CVE-2025-21378 | 7.8 HIGH |
| CVE-2025-21332 | 4.3 MEDIUM |
| CVE-2025-21246 | 8.8 HIGH |

| | |
|---|---|
| CVE-2025-21417 | 8.8 HIGH |
| CVE-2025-21250 | 8.8 HIGH |
| CVE-2025-21240 | 8.8 HIGH |
| CVE-2025-21238 | 8.8 HIGH |
| CVE-2025-21223 | 8.8 HIGH |
| CVE-2025-21409 | 8.8 HIGH |
| CVE-2025-21245 | 8.8 HIGH |
| CVE-2025-21297 | 8.1 HIGH |
| CVE-2025-21309 | 8.1 HIGH |
| CVE-2025-21193 | 6.5 MEDIUM |
| CVE-2025-21225 | 5.9 MEDIUM |
| CVE-2025-21218 | 7.5 HIGH |
| CVE-2025-21234 | 7.8 HIGH |
| CVE-2025-21235 | 7.8 HIGH |
| CVE-2025-21224 | 8.1 HIGH |
| CVE-2025-21275 | 7.8 HIGH |
| CVE-2025-21317 | 5.5 MEDIUM |
| CVE-2025-21335 | 7.8 HIGH |
| CVE-2025-21333 | 7.8 HIGH |
| CVE-2025-21334 | 7.8 HIGH |
| CVE-2025-21343 | 7.5 HIGH |
| CVE-2025-21370 | 7.8 HIGH |
| CVE-2025-21315 | 7.8 HIGH |

| | |
|---|---|
| CVE-2025-21372 | 7.8 HIGH |
| CVE-2025-21313 | 6.5 MEDIUM |
| CVE-2025-21326 | 7.8 HIGH |
| CVE-2025-21311 | 9.8 CRITICAL |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-591 | Sensitive Data Storage in Improperly Locked Memory |
| CWE-636 | Not Failing Securely ('Failing Open') |
| CWE-59 | Improper Link Resolution Before File Access ('Link Following') |
| CWE-922 | Insecure Storage of Sensitive Information |
| CWE-191 | Integer Underflow (Wrap or Wraparound) |
| CWE-126 | Buffer Over-read |
| CWE-303 | Incorrect Implementation of Authentication Algorithm |
| CWE-41 | Improper Resolution of Path Equivalence |
| CWE-415 | Double Free |
| CWE-908 | Use of Uninitialized Resource |
| CWE-843 | Access of Resource Using Incompatible Type ('Type Confusion') |
| CWE-833 | Deadlock |
| CWE-190 | Integer Overflow or Wraparound |
| CWE-693 | Protection Mechanism Failure |
| CWE-532 | Insertion of Sensitive Information into Log File |
| CWE-451 | User Interface (UI) Misrepresentation of Critical Information |
| CWE-285 | Improper Authorization |
| CWE-362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |

| | |
|---|---|
| CWE-125 | Out-of-bounds Read |
| CWE-352 | Cross-Site Request Forgery (CSRF) |
| CWE-284 | Improper Access Control |
| CWE-416 | Use After Free |
| CWE-476 | NULL Pointer Dereference |
| CWE-94 | Improper Control of Generation of Code ('Code Injection') |
| CWE-400 | Uncontrolled Resource Consumption |
| CWE-200 | Exposure of Sensitive Information to an Unauthorized Actor |
| CWE-122 | Heap-based Buffer Overflow |

## Getroffen producten

| **microsoft** |
|---|
| windows_10_version_1507 |
| windows_10_version_1607 |
| windows_10_version_1809 |
| windows_10_version_21h2 |
| windows_10_version_22h2 |
| windows_11_version_22h2 |
| windows_11_version_22h3 |
| windows_11_version_23h2 |
| windows_11_version_24h2 |
| windows_server_2008__service_pack_2 |
| windows_server_2008_r2_service_pack_1 |
| windows_server_2008_r2_service_pack_1__server_core_installation_ |
| windows_server_2008_service_pack_2 |

| |
|---|
| windows_server_2008_service_pack_2__server_core_installation_ |
| windows_server_2012 |
| windows_server_2012__server_core_installation_ |
| windows_server_2012_r2 |
| windows_server_2012_r2__server_core_installation_ |
| windows_server_2016 |
| windows_server_2016__server_core_installation_ |
| windows_server_2019 |
| windows_server_2019__server_core_installation_ |
| windows_server_2022 |
| windows_server_2022__23h2_edition__server_core_installation_ |
| windows_server_2025 |
| windows_server_2025__server_core_installation_ |

## Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.