

A decorative graphic on the left side of the slide, consisting of a network of light blue lines and circles resembling a circuit board or data flow.

# VULNERABILITÀ PIÙ RECENTI

ANALISI CONDOTTA DA:  
LUISA MELE



# VULNERABILITÀ NOTE PIÙ RECENTI

CVE-2025-22467: Vulnerabilità di overflow del buffer nello stack, che consente l'esecuzione di codice remoto da parte di un aggressore autenticato con privilegi limitati.

Fonte: <https://www.redhotcyber.com/post/ivanti-nel-mirino-la-vulnerabilita-con-cvss-9-9-potrebbe-essere-sfruttata-a-breve>

- CVE-2025-23114: Falla nel software di backup, che potrebbe permettere a un attaccante di eseguire codice arbitrario tramite un attacco "Man-in-the-Middle».

Fonte: <https://www.integrity360.com/it/en-us/resources/threat-intel-roundup/threat-intel-roundup-7-2-25>

- CVE-2025-21293: Una vulnerabilità di escalation dei privilegi in Active Directory, sfruttabile per ottenere accesso a livello di sistema all'interno di un ambiente Active Directory.

Fonte: <https://prothect.it/vulnerabilita/exploit-cve-2025-21293-active-directory>

- Zero-day in Microsoft (febbraio 2025): Nel Patch Tuesday di febbraio 2025, Microsoft ha corretto quattro vulnerabilità zero-day, di cui due già attivamente sfruttate in rete.

- Fonte: <https://www.cybersecurity360.it/nuove-minacce/un-patch-tuesday-leggero-quello-di-febbraio-2025-ma-con-quattro-zero-day-corrette>

# CVE-2025-21293

- Vulnerabilità che impatta i servizi di Active Directory Domain Services (AD DS) di Microsoft.

Permette un privilege escalation, tramite la modifica dei permessi in un gruppo chiamato "Network Configuration Operators", al fine di modificare la configurazione di rete e creare una libreria di sistema tramite l'accesso a chiavi di registro.

La vulnerabilità consente l'esecuzione di codice tramite librerie di sistema.

## CVE-2025-21293 Detail

### Description

Active Directory Domain Services Elevation of Privilege Vulnerability

### Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

#### CVSS 3.x Severity and Vector Strings:




**CNA:** Microsoft Corporation

**Base Score:** 8.8 HIGH

**Vector:**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



## REMEDIATION PER LA VULNERABILITÀ CVE-2025- 21293

### Remediation:

- Aggiornare Windows e i server Active Directory il prima possibile con le patch di gennaio 2025.
- Limitare i permessi del gruppo "Network Configuration Operators" per ridurre il rischio di attacco.

## CVE-2025-22467 Detail

### Description

A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.6 allows a remote authenticated attacker to achieve remote code execution.

### Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

#### CVSS 3.x Severity and Vector Strings:



**NIST:** NVD

**Base Score:** 8.8 HIGH

**Vector:**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



**CNA:** ivanti

**Base Score:**

9.9 CRITICAL

**Vector:**

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

## CVE-2025-22467:

- Ivanti Connect Secure (ICS) è una soluzione VPN SSL (Secure Sockets Layer) e Zero Trust Network Access (ZTNA).

La vulnerabilità CVE-2025-22467 impatta Ivanti Connect Secure,.

Nelle versioni del software precedenti alla 22.7R2.6, c'è un errore che può portare a un overflow del buffer basato su stack,

Avendo accesso ai sistemi, sfruttare questa vulnerabilità significa che si potrebbero lanciare comandi da remoto.



## REMEDIATION PER LA VULNERABILITÀ CVE-2025- 22467

Vulnerabilità già patchata.

### Remediation:

Aggiornamento a Ivanti Connect Secure alla versione 22.7R2.6 o successiva.

# CVE-2025-23114:

- Questa CVE impatta i server Veeam che distribuiscono aggiornamenti a diversi servizi come Google, AWS, Oracle.

Lo sfruttamento di questa vulnerabilità consente di eseguire codice arbitrario tramite Man in The Middle.

Il problema deriva da una mancata validazione adeguata dei certificati TLS durante il processo di aggiornamento.

## CVE-2025-23114 Detail

### AWAITING ANALYSIS

This CVE record has been marked for NVD enrichment efforts.

### Description

A vulnerability in Veeam Updater component allows Man-in-the-Middle attackers to execute arbitrary code on the affected server. This issue occurs due to a failure to properly validate TLS certificate.

### Metrics

CVSS Version 4.0

CVSS Version 3.x

CVSS Version 2.0

*NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.*

#### CVSS 3.x Severity and Vector Strings:



**NIST:** NVD

**Base Score:** N/A

NVD assessment not yet provided.



**CNA:** HackerOne


**Base Score:**

9.0 CRITICAL

**Vector:**

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H





# REMEDIATION PER LA VULNERABILITÀ CVE-2025- 23114

- [Vulnerabilità già patchata.](#)

## Remediation:

Aggiornamento del componente Veeam Updater:

Veeam Backup for Salesforce: versione 7.9.0.1124.

Veeam Backup for Nutanix AHV: versione 9.0.0.1125.

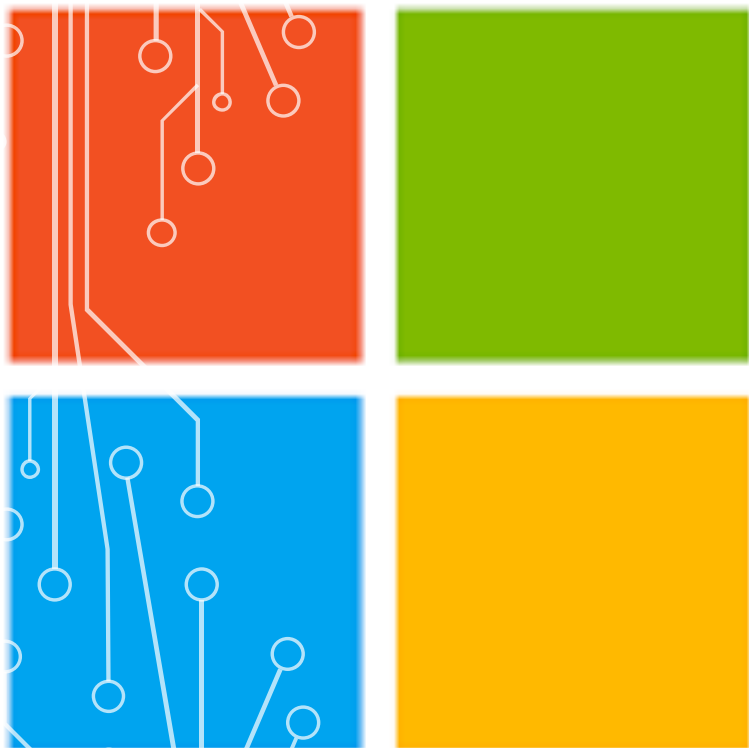
Backup for AWS: versione 9.0.0.1126.

Backup for Microsoft Azure: versione 9.0.0.1128.

Veeam Backup for Google Cloud: versione 9.0.0.1128.

Veeam Backup for Oracle Linux Virtualization Manager e Red Hat Virtualization: versione 9.0.0.1127.





# ZERO-DAY IN MICROSOFT (FEBBRAIO 2025):

Nel febbraio 2025, Microsoft ha rilasciato aggiornamenti per risolvere 56 vulnerabilità, tra cui quattro zero-day, due delle quali attivamente sfruttate:

- CVE-2025-21418: vulnerabilità nel driver di funzione ausiliaria di Windows per WinSock che consente a un utente autenticato di eseguire codice con privilegi 'SYSTEM'.
- CVE-2025-21391: vulnerabilità in Windows Storage che di eliminare file mirati, causando l'indisponibilità del servizio.
- CVE-2025-21194: vulnerabilità nei dispositivi Microsoft Surface che potrebbe compromettere l'hypervisor e il kernel.
- CVE-2025-21377: vulnerabilità che sfrutta lo spoofing, esponendo gli hash NTLMv2 degli utenti, facilitando attacchi di autenticazione.

Microsoft consiglia come remediation l'aggiornamento tempestivo degli applicativi.

A decorative graphic on the left side of the slide, consisting of a network of light blue lines and circles. The lines are vertical and horizontal, with some diagonal segments, and the circles are small and white, resembling nodes or components of a circuit.

**GRAZIE!**