REPORT SULLE VULNERABILITÀ CVE DI WINDOWS 10

1. Introduzione Windows 10 ha registrato numerose vulnerabilità nel corso degli anni, molte delle quali identificate attraverso il sistema di classificazione CVE (Common Vulnerabilities and Exposures). Questo report fornisce un elenco di alcune delle principali vulnerabilità riscontrate, con una descrizione dei problemi e delle soluzioni consigliate.

2. Elenco delle principali CVE di Windows 10

- **CVE-2018-0775**: Una vulnerabilità in Microsoft Edge (Windows 10 versione 1709) consente l'esecuzione di codice arbitrario a causa di una gestione errata degli oggetti in memoria da parte del motore di scripting.

- **CVE-2018-0774**: Simile alla precedente, questa vulnerabilità riguarda Microsoft Edge e può essere sfruttata per eseguire codice arbitrario.

- **CVE-2018-0773**: Un'altra vulnerabilità in Microsoft Edge che consente l'esecuzione di codice arbitrario nel contesto dell'utente corrente, dovuta alla gestione degli oggetti in memoria.

- **CVE-2018-0772**: Questa vulnerabilità riguarda Internet Explorer e permette a un attaccante di eseguire codice arbitrario nel contesto dell'utente corrente.

- **CVE-2018-0770**: Una vulnerabilità in Microsoft Edge che consente l'esecuzione di codice arbitrario a causa di una cattiva gestione della memoria.

- **CVE-2024-43491**: Identificata nel settembre 2024, questa vulnerabilità riguarda una falla nel Servicing Stack di Windows 10 versione 1507, che ha causato il rollback delle correzioni per alcune vulnerabilità, rendendo il sistema vulnerabile agli attacchi.

3. Impatti e Rischi Le vulnerabilità sopra elencate possono essere sfruttate da attaccanti per:

- Eseguire codice arbitrario sul sistema target;
- Ottenere privilegi elevati;
- Compromettere la sicurezza dei dati;
- Installare malware o ransomware;
- Eseguire attacchi di tipo Remote Code Execution (RCE).

4. Soluzioni e Mitigazioni Per proteggersi dalle vulnerabilità sopra indicate, si consiglia di:

- Installare regolarmente le patch di sicurezza rilasciate da Microsoft;
- Evitare di utilizzare versioni non aggiornate di Windows 10;
- Abilitare e mantenere aggiornato il software antivirus e antimalware;
- Monitorare le fonti ufficiali di sicurezza per eventuali nuove minacce e aggiornamenti (es. NVD e MITRE CVE).

5. Conclusione Il supporto ufficiale per Windows 10 terminerà il 14 ottobre 2025. Pertanto, oltre a mantenere il sistema operativo aggiornato, è consigliabile pianificare la migrazione a una versione più recente per garantire una protezione continua e ridurre il rischio di attacchi informatici.

Fonti:

- NVD - National Vulnerability Database
- MITRE CVE Database
- Microsoft Security Updates

Questo report fornisce una panoramica delle principali vulnerabilità di Windows 10 e delle misure consigliate per mitigare i rischi associati. Mantenere aggiornato il sistema operativo e adottare buone pratiche di sicurezza informatica è essenziale per proteggere i dati e prevenire attacchi malevoli.