DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

ALERTĂ

01.03.2024

Vulnerabilitate zero-day Windows exploatată de către gruparea de atacatori Lazarus

Gruparea Lazarus (alias Hidden Cobra[1]) afiliată statului Nord-Coreean[2] exploatează activ o vulnerabilitate de tip Zero-Day în sistemul de operare Windows pentru a compromite datele utilizatorilor.

Vulnerabilitatea identificată ca CVE-2024-21338 afectează driverul AppLocker al Windows (appid.sys).

Descriere

Vulnerabilitatea permite atacatorilor acces la nivel de nucleu al sistemului de operare și dezactivarea instrumentelor de securitate, eschivând tehnicile zgomotoase BYOVD (Bring Your Own Vulnerable Driver).

Pentru a realiza atacuri mai subtile și a consolida prezența pe sistemele compromise este folosită o versiune actualizată a rootkit-ului FudModule, cu îmbunătățiri semnificative privind exfiltrarea și funcționalitatea, inclusiv mecanisme de dezactivare a soluțiilor de securitate precum Microsoft Defender, CrowdStrike Falcon și HitmanPro.

În prezent, vulnerabilitatea este exploatată de către gruparea Lazarus (alias APT38, APT-C-26, ATK117, ATK3, Andariel, Appleworm, Bluenoroff, Bureau 121, COPERNICIUM, COVELLITE, Citrine Sleet, DEV-0139, DEV-1222, Dark Seoul, Diamond Sleet, G0032, G0082, Genie Spider, Group 77, Hastati Group, Labyrinth Chollima, NICKEL GLADSTONE, NewRomanic Cyber Army Team, Nickel Academy, Operation AppleJeus, Operation DarkSeoul, Operation GhostSecret, Operation Troy, Sapphire Sleet, Stardust Chollima, Subgroup: Bluenoroff, TA404, Unit 121, Whois Hacking Team, ZINC, Zinc[3]), cunoscută pentru atacurile motivate financiar și afilierea cu Coreea de Nord.

Impact

Compania multinațională cehă de securitate cibernetică **Avast** a descoperit și raportat[4] vulnerabilitatea care a fost ulterior remediată de Microsoft în **actualizarea Patch Tuesday din februarie 2024**[5]. Exploatarea implică manipularea avansată a obiectelor kernel și evidențiază o evoluție semnificativă a tehnicilor de atac, marcând o trecere de la exploatarea driverelor terțe vulnerabile la exploatarea vulnerabilităților zero-day în driverele native Windows. Aceasta a demonstrat o capacitate crescută de exfiltrare și rezistență în fața eforturilor de detecție, însoțită de introducerea unui nou troian de acces la distanță (RAT) pentru a facilita controlul de la distanță al sistemelor compromise.

Potențialele efecte ar implica posibilitatea compromiterii integrității sistemului, pierderea confidențialității datelor și încălcarea securității proceselor critice, afectând în mod direct organizațiile vizate și ridicând preocupări majore pentru comunitatea de securitate cibernetică.

---

[1] Lazarus Group, Labyrinth Chollima, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY, Group G0032 | MITRE ATT&CK®

[3] Lazarus Group (Threat Actor) (fraunhofer.de)

[4] Lazarus and the FudModule Rootkit: Beyond BYOVD with an Admin-to-Kernel Zero-Day - Avast Threat Labs

[5] February 2024 Security Updates - Release Notes - Security Update Guide - Microsoft

Remediere

Echipa Directoratului Național de Securitate Cibernetică (DNSC) recomandă aplicarea imediată a actualizărilor de securitate furnizate prin Microsoft în Patch Tuesday din luna februarie 2024 pentru a mitiga riscul de exploatare.

Totodată, organizațiile sunt, încurajate să revizuiască și să întărească politicile de securitate, să monitorizeze activitatea rețelei pentru indicatori de compromitere și să implementeze soluții avansate de detecție și răspuns.

Pentru consultarea listei de indicatori de compromitere, precum și alte detalii tehnice ale vulnerabilității, se poate consulta acest material.

Reguli YARA

ioc/FudModule at master · avast/ioc · GitHub

Surse

Lazarus and the FudModule Rootkit: Beyond BYOVD with an Admin-to-Kernel Zero-Day - Avast Threat Labs

Lazarus hackers exploited Windows zero-day to gain Kernel privileges (bleepingcomputer.com)

North Korean hackers exploit Windows zero-day flaw (therecord.media)

alerts@dnsc.ro

Telefon 1911

#DNSC #alert #cybersecurity #awareness