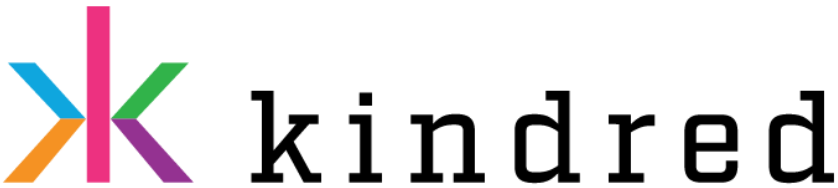

Security Newsletter

15 June 2020

Subscribe to this newsletter

SMBleed: A New Critical Vulnerability Affects Windows SMB Protocol

Cybersecurity researchers today uncovered a new critical vulnerability affecting the Server Message Block (SMB) protocol that could allow attackers to leak kernel memory remotely, and when combined with a previously disclosed "wormable" bug, the flaw can be exploited to achieve remote code execution attacks.

Dubbed "SMBleed" (CVE-2020-1206) by cybersecurity firm ZecOps, the flaw resides in SMB's decompression function — the same function as with SMBGhost or EternalDarkness bug (CVE-2020-0796), which came to light three months ago, potentially opening vulnerable Windows systems to malware attacks that can propagate across networks. The newly discovered vulnerability impacts Windows 10 versions 1903 and 1909, for which Microsoft today released security patches as part of its monthly Patch Tuesday updates for June.

To mitigate the vulnerability, it's recommended that home and business users install the latest Windows updates as soon as possible. For systems where the patch is not applicable, it's advised to block port 445 to prevent lateral movement and remote exploitation.

Read More on TheHackerNews

Even More on BleepingComputer

More #News

- Jenkins team avoids security disaster after partial user database loss
- Gamaredon hackers use Outlook macros to spread malware to contacts
- Facebook Helped the FBI Hack a Child Predator
- Live event solutions leader TAIT discloses data breach
- Fortune 500 insurance firm Genworth discloses data breach
- Microsoft discovers cryptomining gang hijacking Kubernetes clusters
- FBI warns of increased hacking risk if using mobile banking apps
- Honda Confirms Hack Attack Disrupted Global Production
- Nintendo Says 300,000 Accounts Breached After Hack
- Windows Group Policy flaw lets attackers gain admin privileges
- Security Drift – The Silent Killer
- Magecart Targets Emergency Services-related Sites via Insecure S3 Buckets
- Apple hopes to bolster password security with open source project
- Hackers are attacking the German PPE supply chain
- CallStranger vulnerability lets attacks bypass security systems and scan LANs
- Cyber incidents at NASA spiked 366% in 2019

#Patch Time!

- Microsoft Patch Tuesday, June 2020 Edition
- Vulnerabilities in popular open source projects doubled in 2019
- Google Researcher Finds Vulnerability in VMware Virtualization Products
- Billions of devices affected by UPnP vulnerability
- Intel patched 22 vulnerabilities in the June 2020 Platform Update
- Adobe fixes critical remote code execution bug in Flash Player

#Tech and #Tools

- Is Your Database Secured? Think Again
- Understanding Web Security Checks in Firefox (Part 1)
- Anatomy of Automated Account Takeovers
- Introduction to Cross-Site Request Forgery (CSRF)
- Group Policies Going Rogue
- PatchChecker: Web-based check for Windows privesc vulnerabilities
- Abusing Windows telemetry for persistence
- How to investigate anomaly detection alerts
- Applied Purple Teaming - Infrastructure, Threat Optics, and Continuous Improvement
- Automating the provisioning of Active Directory labs in Azure
- Red Team: Using SharpChisel to exfil internal networ
- The Impending Doom of Expiring Root CAs and Legacy Clients

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us