kindred

Security Newsletter

19 August 2019

Subscribe to this newsletter

4 New BlueKeep-like 'Wormable' Windows Remote Desktop Flaws Discovered

If you are using any supported version of the Windows operating system, stop everything and install the latest security updates from Microsoft immediately. Windows operating system contains four new critical wormable, remote code execution vulnerabilities in Remote Desktop Services, similar to the recently patched 'BlueKeep' RDP vulnerability.

Discovered by Microsoft's security team itself, all four vulnerabilities, CVE-2019-1181, CVE-2019-1182, CVE-2019-1222, and CVE-2019-1226, can be exploited by unauthenticated, remote attackers to take control of an affected computer system without requiring any user interaction. Just like BlueKeep RDP flaw, all four newly discovered vulnerabilities are also wormable and could be exploited by potential malware to propagate itself from one vulnerable computer to another automatically.

Besides these four critical security flaws, Microsoft has also patched 89 vulnerabilities as part of the company's monthly batch of software security updates for August, 25 of which are rated critical and 64 important in severity.

Read More on TheHackerNews

8 New HTTP/2 Implementation Flaws Expose Websites to DoS Attacks

Various implementations of HTTP/2, the latest version of the HTTP network protocol, have been found vulnerable to multiple security vulnerabilities affecting the most popular web server software, including Apache, Microsoft's IIS, and NGINX.

Launched in May 2015, HTTP/2 has been designed for better security and improved online experience by speeding up page loads. Today, over hundreds of millions of websites, or some 40 percent of all the sites on the Internet, are running using HTTP/2 protocol. A total of eight high-severity HTTP/2 vulnerabilities, seven discovered by Jonathan Looney of Netflix and one by Piotr Sikora of Google, exist due to resource exhaustion when handling malicious input, allowing a client to overload server's queue management code.

However, it should be noted that the vulnerabilities can only be used to cause a DoS condition and do not allow attackers to compromise the confidentiality or integrity of the data contained within the vulnerable servers. According to CERT, affected vendors include NGINX, Apache, H2O, Nghttp2, Microsoft (IIS), Cloudflare, Akamai, Apple (SwiftNIO), Amazon, Facebook (Proxygen), Node.js, and Envoy proxy, many of which have already released security patches and advisories.

Read More on TheHackerNews

Even More on BleepingComputer

More #News

- 'NULL' license plate gets security researcher $12K in tickets
- 5 Things to Know About Cyber Insurance
- Meet Bluetana, the Scourge of Pump Skimmers
- Extended Validation Certificates are (Really, Really) Dead

- Choice Hotels: 700,000 Guest Records Exposed
- Android Users Can Now Log in to Google Services Using Fingerprint
- Google Has Started Removing FTP Support From Chrome
- Hacking forum spills rival's 321,000 member database
- Four major dating apps expose precise locations of 10 million users
- New Norman Cryptominer Uses Dynamic DNS for C2 Communication
- Exploiting GDPR to Get Private Information
- Pwnie Awards 2019 Winners
- Free MANRS Tool Helps Improve Routing Security
- SQLite Vulnerability Permits iOS Hack: Report
- Annual Research from WhiteHat Security Says Remediation Rates for App Vulnerabilities Continue to Fall
- New Bluetooth KNOB Attack Lets Attackers Manipulate Traffic
- Hundreds of exposed Amazon cloud backups found leaking sensitive data
- Repurposing Mac Malware Not Difficult, Researcher Shows
- Hidden Injection Flaws Found in BIG-IP Load Balancers
- Microsoft Office Phishers Move to Enterprise AWS Landing Pages

#Patch Time!

- Patch Tuesday, August 2019 Edition
- HTTP/2 Denial of Service Advisory
- Windows 10 Security Alert: Vulnerabilities Found in Over 40 Drivers
- Patches for 2 Severe LibreOffice Flaws Bypassed — Update to Patch Again
- Many Apache Struts Security Advisories Updated Following Review
- Windows CTF Flaws Enable Attackers to Fully Compromise Systems
- SAP Patches Highest Number of Critical Flaws Since 2014
- Firefox fixes "master password" security bypass bug
- Steam Security Vulnerability Fixed, Researchers Don't Agree

#Tech and #Tools

- Kubernetes Pod Security Policy Best Practices
- Offensive Lateral Movement
- Huge Survey of Firmware Finds No Security Gains in 15 Years
- SSRF (Server Side Request Forgery) interrative tutorial
- How to change a root password in a Docker image
- Public Exploits RSS Feed
- Down the Rabbit-Hole...
- Generating Personalized Wordlists with NLP For Password Guessing Attacks
- Say Cheese: Ransomware-ing a DSLR Camera
- Making it Rain shells in Kubernetes
- Commando VM 2.0: Customization, Containers, and Kali, Oh My!
- Active Defense - Dynamically Locking AWS Credentials to Your Environment
- SILENTTRINITY: multiserver/multiuser open source C2

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. You can find all our open vacancies on our career page.

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 over 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

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