kindred

Security Newsletter

10 May 2021

Subscribe to this newsletter

21Nails: Multiple Critical Vulnerabilities in Exim Mail Server

Newly discovered critical vulnerabilities in the Exim mail transfer agent (MTA) software allow unauthenticated remote attackers to execute arbitrary code and gain root privilege on mail servers with default or common configurations.

The security flaws (10 remotely exploitable and 11 locally) found and reported by the Qualys Research Team are collectively known as 21Nails.

One of the vulnerabilities discovered affects all versions of Exim going back all the way to 2004 (going back to the beginning of its Git history 17 years ago).

Read More on Qualys blog

More #News

- Crypto miners are killing free CI
- Cloud Incident Response Framework
- How China turned a prize-winning iPhone hack against the Uyghurs
- Malicious Office 365 Apps Are the Ultimate Insiders
- Google Wants to Make Everyone Use Two Factor Authentication
- Chinese military unit accused of cyber-espionage bought multiple western antivirus products
- Bulletproof hosting admins plead guilty to running cybercrime safe haven
- New TsuNAME DNS bug allows attackers to DDoS authoritative DNS servers
- Your Old Phone Number Can Be Used to Hack You
- Apple Is Having a Really Bad Time With iPhone Security Bugs This Year

- New Attacks Slaughter All Spectre Defenses

#Breach Log

- A student pirating software led to a full-blown Ryuk ransomware attack
- Largest U.S. pipeline shuts down operations after ransomware attack
- Business email compromise campaign targets wide range of orgs with gift card scam
- Twilio discloses impact from Codecov supply-chain attack
- Health care giant Scripps Health hit by ransomware attack
- Ransomware Hits Australian Telecom Provider Telstra's Partner

#Patch Time!

- Dell patches 12-year-old driver vulnerability impacting millions of PCs
- Cisco HyperFlex HX Command Injection Vulnerabilities
- Foxit Reader bug lets attackers run malicious code via PDFs
- Qualcomm vulnerability impacts nearly 40% of all mobile phones
- Cisco bugs allow creating admin accounts, executing commands as root
- VMware fixes critical RCE bug in vRealize Business for Cloud
- Google Chrome adopts Windows 10 exploit protection feature
- Apple fixes 2 iOS zero-day vulnerabilities actively used in attacks
- Pulse Secure fixes VPN zero-day used to hack high-value targets
- Firefox for Android gets critical update to block cookie-stealing hole

#Tech and #Tools

- Trickbot Brief: Creds and Beacons
- Relaying Potatoes: Another Unexpected Privilege Escalation Vulnerability in Windows RPC Protocol
- Jenkins Attack Framework
- Mystikal - Addressing the pain of macOS initial access payloads
- RM3 – Curiosities of the wildest banking malware
- Bypassing EDR real-time injection detection logic
- HoneyCreds - Catching Network Poisoners Like Responder
- Domain Hijacking Via Logic Error

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