kindred

Security Newsletter

9 September 2019

Subscribe to this newsletter

Exim TLS Flaw Opens Email Servers to Remote 'Root' Code Execution Attacks

A critical remote code execution vulnerability has been discovered in the popular open-source Exim email server software, leaving at least over half a million email servers vulnerable to remote hackers. Exim is a widely used, open source mail transfer agent (MTA) software developed for Unix-like operating systems such as Linux, Mac OSX or Solaris, which runs almost 60% of the internet's email servers today for routing, delivering and receiving email messages.

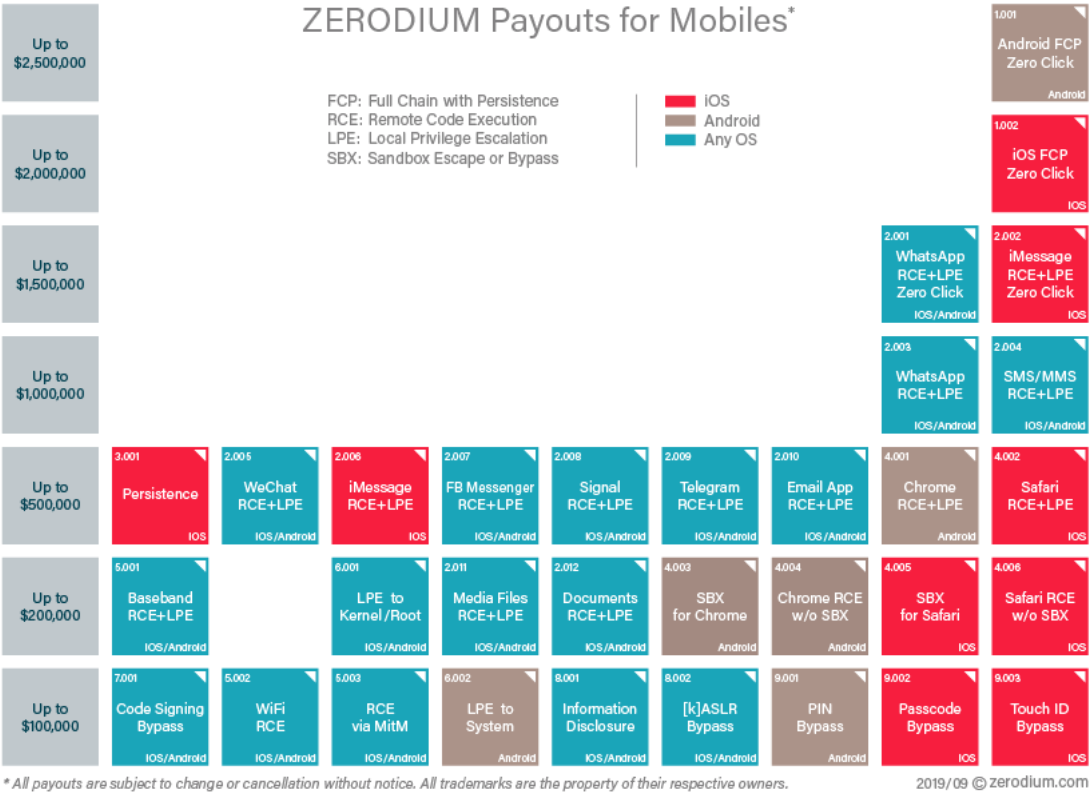
Exim maintainers today released Exim version 4.92.2 after publishing an early warning two days ago, giving system administrators a heads-up on its upcoming security patches that affect all versions of the email server software up to and including then-latest 4.92.1.

Just three months ago, Exim also patched a severe remote command execution vulnerability, tracked as CVE-2019-10149, that was actively exploited in the wild by various groups of hackers to compromise vulnerable servers. The Exim advisory says that a rudimentary proof of concept (PoC) exists for this flaw, but currently there is no known exploit available to the public. Server administrators are highly recommended to install the latest Exim 4.92.2 version immediately, and if not possible, can mitigate the issue by not allowing unpatched Exim servers to accept TLS connections.

Read More on TheHackerNews

Even More on BleepingComputer

Exploit Reseller Offering Up To $2.5 Million For Android Zero-Days



ZERODIUM Payouts for Mobiles*

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
▨ Android
🟦 Any OS

Up to $2,500,000										1.001 Android FCP Zero Click Android
Up to $2,000,000										1.002 iOS FCP Zero Click iOS
Up to $1,500,000									2.001 WhatsApp RCE+LPE Zero Click iOS/Android	2.002 iMessage RCE+LPE Zero Click iOS
Up to $1,000,000									2.003 WhatsApp RCE+LPE iOS/Android	2.004 SMS/MMS RCE+LPE iOS/Android
Up to $500,000	3.001 Persistence iOS	2.005 WeChat RCE+LPE iOS/Android	2.006 iMessage RCE+LPE iOS	2.007 FB Messenger RCE+LPE iOS/Android	2.008 Signal RCE+LPE iOS/Android	2.009 Telegram RCE+LPE iOS/Android	2.010 Email App RCE+LPE iOS/Android	4.001 Chrome RCE+LPE Android	4.002 Safari RCE+LPE iOS
Up to $200,000	5.001 Baseband RCE+LPE iOS/Android		6.001 LPE to Kernel/Root iOS/Android	2.011 Media Files RCE+LPE iOS/Android	2.012 Documents RCE+LPE iOS/Android	4.003 SBX for Chrome Android	4.004 Chrome RCE w/o SBX Android	4.005 SBX for Safari iOS	4.006 Safari RCE w/o SBX iOS
Up to $100,000	7.001 Code Signing Bypass iOS/Android	5.002 WiFi RCE iOS/Android	5.003 RCE via MitM iOS/Android	6.002 LPE to System Android	8.001 Information Disclosure iOS/Android	8.002 [k]ASLR Bypass iOS/Android	9.001 PIN Bypass Android	9.002 Passcode Bypass iOS	9.003 Touch ID Bypass iOS

*All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

The zero-day buying and selling industry has recently taken a shift towards Android operating system, offering up to $2.5 million payouts to anyone who sells 'full chain, zero-click, with persistence' Android zero-days. Zerodium is a startup that buys zero-day exploits from hackers, and then probably sells them to law enforcement agencies and nation-sponsored spies around the world.

Just like other traditional markets, the zero-day market is also a game of supply, demand, and strategy, which suggests either the demand of Android zero-days has significantly increased or somehow Android OS is getting tougher to hack remotely, which is unlikely.

While the same type of zero-day exploits for iOS devices are worth $2 million, which is still double than what Apple has recently started offering to hackers to responsibly report severe deadly exploits, described as "a zero-click kernel code execution vulnerability that enables complete, persistent control of a device's kernel."

Read More on TheHackerNews

Zerodium Payouts

More #News

- Spam In your Calendar? Here's What to Do.
- XKCD Forum Hacked — Over 562,000 Users' Account Details Leaked

- XKCD Forum Hacked — Over 562,000 Users' Account Details Leaked
- Android SMS Phishing Can Stealthily Enable Malicious Settings
- Over 47,000 Supermicro servers are exposing BMC ports on the internet
- Hacked SharePoint Sites Used to Bypass Secure Email Gateways
- Foxit PDF Software Company Suffers Data Breach—Asks Users to Reset Password
- Mozilla Will Support Existing Ad Blockers in Extensions Manifest v3
- Cisco releases guides for incident responders handling hacked Cisco gear
- A Summer of Discontent: The Hottest Malware Hits
- Database exposed 133 million US Facebook users' phone numbers
- Windows and AV Software Ignore Malware in Virtual Disk Files
- A Chinese APT is now going after Pulse Secure and Fortinet VPN servers
- Twitter temporarily disables 'Tweeting via SMS' after CEO gets hacked
- Google Chrome Starts Testing Third-Party Cookie Blocking
- New Toolkit Pushes Malware via Fake Program Update Alerts in 30 Languages
- Brave uncovers Google's GDPR workaround

#Patch Time!

- Exim - CVE-2019-15846
- Firefox 69 Patches Critical Code Execution Flaw
- Microsoft Releases September 2019 Office Updates With Fixes, Improvements
- Multiple Code Execution Flaws Found In PHP Programming Language
- Cisco Patches Remote Command Execution in Webex Teams Client
- WordPress 5.2.3 Released with Security and Bug Fixes

#Tech and #Tools

- CSRF is (really) dead - SameSite default on Chrome
- DNS Spoofing on Kubernetes Clusters
- Security analysis of portal element
- Exim servers - Shodan
- ThreatGEN: Red vs. Blue (VideoGame)
- Hardening Your Azure Domain Front
- SharPersist: Windows Persistence Toolkit in C#
- ObscurityLabs RedTeam C# Toolkit
- How To: Restrict RDP Access to AD Domain Controllers via IPSec, GPOs, and WFAS
- A brief analysis of data compression security issues
- Red Teamer's Guide to Pulse Secure SSL VPN
- Bitbucket 6.1.1 Path Traversal to RCE
- How to build an internal red team?
- Gaining Persistency on Vulnerable Lambdas
- Analysis of Common Federated Identity Protocols
- MWR Labs: C3 - First Look
- Custom Command and Control (C3)

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