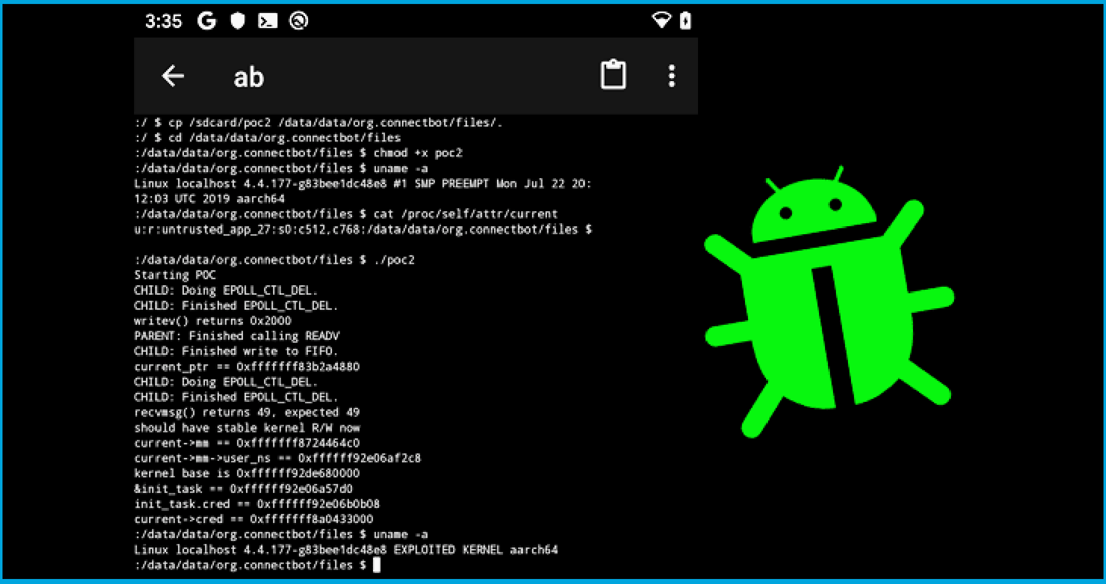
kindred

Security Newsletter

7 October 2019

Subscribe to this newsletter

New 0-Day Flaw Affecting Most Android Phones Being Exploited in the Wild



```
:/ $ cp /sdcard/poc2 /data/data/org.connectbot/files/.
:/ $ cd /data/data/org.connectbot/files
:/data/data/org.connectbot/files $ chmod +x poc2
:/data/data/org.connectbot/files $ uname -a
Linux localhost 4.4.177-g83bee1dc48e8 #1 SMP PREEMPT Mon Jul 22 20:
12:03 UTC 2019 aarch64
:/data/data/org.connectbot/files $ cat /proc/self/attr/current
u:r:untrusted_app_27:s0:c512,c768:/data/data/org.connectbot/files $

:/data/data/org.connectbot/files $ ./poc2
Starting POC
CHILD: Doing EPOLL_CTL_DEL.
CHILD: Finished EPOLL_CTL_DEL.
writev() returns 0x2000
PARENT: Finished calling READV
CHILD: Finished write to FIFO.
current_ptr == 0xffffff83b2a4880
CHILD: Doing EPOLL_CTL_DEL.
CHILD: Finished EPOLL_CTL_DEL.
recvmsg() returns 49, expected 49
should have stable kernel R/W now
current->mm == 0xffffff8724464c0
current->mm->user_ns == 0xffffff92e06af2c8
kernel base is 0xffffff92de680000
&init_task == 0xffffff92e06a57d0
init_task.cred == 0xffffff92e06b0b08
current->cred == 0xffffff8a0433000
:/data/data/org.connectbot/files $ uname -a
Linux localhost 4.4.177-g83bee1dc48e8 EXPLOITED KERNEL aarch64
:/data/data/org.connectbot/files $ █
```

Another day, another revelation of a critical unpatched zero-day vulnerability, this time in the world's most widely used mobile operating system, Android. What's more? The Android zero-day vulnerability has also been found to be exploited in the wild by the Israeli surveillance vendor NSO Group—infamous for selling zero-day exploits to governments—or one of its customers, to gain control of their targets' Android devices.

Discovered by Project Zero researcher Maddie Stone, the details and a proof-of-concept exploit for the high-severity security vulnerability, tracked as CVE-2019-2215, has been made public today—just seven days after reporting it to the Android security team.

According to the researcher, since the issue is "accessible from inside the Chrome sandbox," the Android kernel zero-day vulnerability can also be exploited remotely by combining it with a separate Chrome rendering flaw. "The bug is a local privilege escalation vulnerability that allows for a full compromise of a vulnerable device. If the exploit is delivered via the Web, it only needs to be paired with a renderer exploit, as this vulnerability is accessible through the sandbox," Stone says in the Chromium blog.

Read More on TheHackerNews

Even More on BleepingComputer

Microsoft: MFA bypass attacks are so rare we don't have good statistics on them

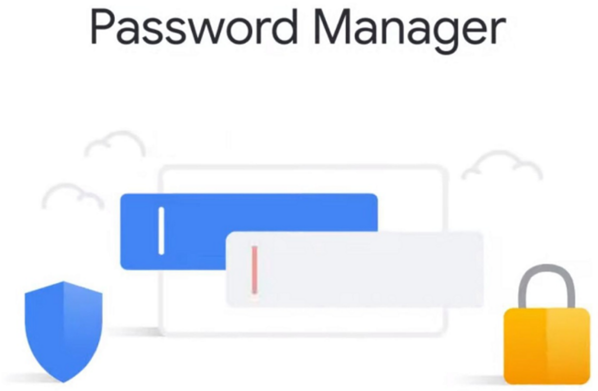
Attacks on Microsoft user accounts that are capable of bypassing multi-factor authentication (MFA) protections are so rare that the Redmond-based company doesn't even have stats for them. "When we evaluate all the tokens issued with MFA claims, we see that less than 10% of users use MFA per month in our enterprise accounts (and that includes on premises and third party MFA)". The Microsoft security expert claims that this slow rate of adoption among Microsoft users is what's kept attackers from evolving and deploying tools that can intercept MFA operations.

But he also warns Microsoft users that tools and methods for bypassing multi-factor authentication exist. For example Modlishka or the educational tool EvilGinx. But the Microsoft security expert doesn't want users to get discouraged from enabling MFA for their accounts just because these tools and techniques exist. As he said before, these attacks are so rare that Microsoft barely sees any. Instead, he recommends that users enable MFA for their accounts, with the strongest authentication factor available, as detailed in the table above in this article.

The only solutions with no known real time hijacking capabilities are the use of smartcards, FIDO token (security keys) or Windows Hello.

Read More on ZDNet

Google's Password Manager now checks for breached credentials



Google launched today a new service called Password Checkup that will check a user's saved passwords if they've been leaked and compromised in breaches at other services. The service is currently available for the Google web dashboard and Android devices, but will also be added to the Chrome browser later this year.

On the web, Password Checkup will be available at passwords.google.com. If Chrome users ever choose to use a Google account with the Chrome browser and then saved passwords in Chrome, this is the website where those passwords are synced to.

To use the new feature, a new button that says "Check Passwords" will be available. Once pressed, Google will take all the user's passwords and check them against an internal database of over four billion user credentials that have been leaked online via breaches at other companies. If a username & password combo is found in this database, Google will warn the user that they need to change the password for that account, as they're at risk of having the account hijacked by hackers.

Read More on NakedSecurity

Even More on ZDNet

More #News

- Minerva attack can recover private keys from smart cards, cryptographic libraries
- Google gets tougher on HTTPS with ban on mixed content
- PDF encryption standard weaknesses uncovered
- EA to give users a free month of Origin Access if they enable 2FA
- 'Lost Files' Data Wiper Poses as a Windows Security Scanner
- Just a GIF Image Could Have Hacked Your Android Phone Using WhatsApp

- Microsoft 365 To Get Tenant-Wide Feature Preventing Info Exposure
- 'Vendor Email Compromise': A New Attack Twist
- Zendesk Discloses Old Data Breach From 2016 Affecting 10,000 Accounts
- American Express Customer Info Accessed by Employee for Possible Fraud
- Former Yahoo Employee Admits Hacking into 6000 Accounts for Sexual Content
- Tax and PII records of 20 million Russians stored without encryption, leaked online
- Microsoft To Offer Windows 7 Extended Security Updates to SMBs
- Academics find eight vulnerabilities in Android's VoIP components
- Data breaches now cost companies an average of $1.41 million
- Mariposa Botnet Author, Darkcode Crime Forum Admin Arrested in Germany
- Medical Practice Closing Permanently After Ransomware Attack
- WebEx, Zoom Meetings Exposed to Snooping via Enumeration Attacks
- NSA on the Future of National Cybersecurity
- Zynga's Breach Notification: How Not to Inform Victims
- Users Need to Consent to Online Tracking Cookies: EU Court
- Under-Detected ODT Files Deliver Common Remote Access Trojans
- PSD2 Authentication Deadline Needs to Be Firmed Up - Now
- Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC
- Linux to get kernel 'lockdown' feature
- Supply-Chain Security and Trust
- Russian hacker group patches Chrome and Firefox to fingerprint TLS traffic
- Australian Govt Issues Android and iOS Security Hardening Guides
- Magecart Impacts Hundreds of Thousands of Websites, Still Growing
- Four U.S. Food Chains Disclose Payment Card Theft via PoS Malware

#Patch Time!

- New Critical Exim Flaw Exposes Email Servers to Remote Attacks — Patch Released
- Urgent/11 Flaws Impact More RTOS Used by Medical, Industrial Devices

#Tech and #Tools

- Eyeballer: Convolutional neural network for analyzing pentest screenshots
- Introducing Venator: A macOS tool for proactive detection
- Understanding and Defending Against Access Token Theft: Finding Alternatives to winlogon.exe
- Security baseline (Sept2019Update) for Windows 10 v1903 and Windows Server v1903
- Security Policy Advisor for Office 365 ProPlus is now Generally Available!
- huskyCI - Performing security tests inside your CI
- HTTP Desync Attacks: what happened next
- Saved by the Shell: Reconstructing Command-Line Activity on MacOS
- How I Passed the AWS Certified Security – Specialty
- Beyond The Security Team
- Detecting and characterizing lateral phishing at scale
- Pushing Left, Like a Boss: Table of Contents

- App Analysis: Bird
- Hacking Voi Scooters: How I Created $100k Worth Of Free Rides
- So you want to learn [Red] teaming?
- Red Teaming with Physical Penetration Testing and Social Engineering
- Checkm8 exploit
- Webcast: Implementing Sysmon and Applocker
- Webcast: The Frugal Girl's Guide to Threat Intelligence
- New SIM attacks de-mystified, protection tools now available
- Zero Trust Architecture: Draft NIST SP 800-207 Available for Comment
- Phishing users using EvilGinx and bypassing 2FA

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