EFFECTIVE IMMEDIATELY —

Google will pay $1.5 million for the most severe Android exploits

Big bump coincides with investments Google has poured into securing its Pixel phone.

DAN GOODIN - 11/21/2019, 5:00 PM

New Line Cinema

Enlarge

Google will pay up to $1.5 million for the most severe hacks of its Pixel line of Android phones, a more than seven-fold increase over the previous top Android reward, the company said.

Effective immediately, Google will pay $1 million for a "full chain remote code execution exploit with persistence which compromises the Titan M secure element on Pixel devices," the company said in a post published on Thursday. The company will also pay $500,000 for exploits that exfiltrate data out of a Pixel or bypass its lock screen.

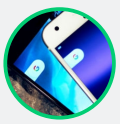
Google will offer a 50 percent bonus to any of its rewards if the exploit works on specific developer preview versions of Android. That means a critical Titan M hack on a developer preview could fetch $1.5 million, and a data exfiltration or lockcscreen bypass on a developer preview could earn $750,000, and so on. Previously, rewards for the most severe Android exploits topped out at $200,000 if they involved the trusted execution environment—an independent OS within Android for handling payments, multi-factor authentication, and other sensitive functions—and $150,000 if they involved compromise only on the Android kernel.

Putting Titan M to the test

The big reward bump coincides with the investments Google has poured into securing the Pixel. The Titan M is a Google-designed chip that's physically segregated from the main chipset of the device. In many respects, it's analogous to the Secure Enclave in iPhones or the TrustZone in devices running an Arm processor. The Titan M is a mobile version of the Titan chip Google introduced in 2017.

The Titan M carries out four core functions, including:

- Storing the last known safe version of Android to ensure hackers can't cause the bootloader—which is the program that validates and loads Android when the phone turns on—to call a malicious or out-of-date version
- Verifying the lock screen passcode or pattern, limiting the number of unsuccessful login attempts that can be made, and securing the device's disk encryption key
- Storing private keys and securing sensitive operations of third-party apps, such as those used to make payments
- Preventing changes to the firmware unless a passcode or pattern is entered

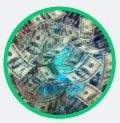


FURTHER READING
Attackers exploit 0-day vulnerability that gives full control of Android phones

Titan M was first introduced in 2018 with the roll out of the Pixel 3. It's also in the recently released Pixel 3a, and will also be included in the just-released Pixel 4. Pixel 2 models relied on a less robust dedicated tamper-resistant hardware security module. In-the-wild exploits disclosed last month were able to remotely execute malicious code on an array of Android phones, including the Pixel 1, Pixel 1 XL, Pixel 2, and Pixel 2 XL, but not the Pixel 3. The Titan M wasn't

responsible for stopping that attack, however. Instead, the reason was that the Pixel 3 and 3a received Linux patches that the vulnerable Pixels had not.

In the four years since the Android Security Rewards Program was introduced, it has paid out more than $4 million from more than 1,800 reports. More than $1.5 million of that came in the past 12 months. The top reward this year was $161,337, which was paid to Guang Gong of Qihoo 360 Technology's Alpha Lab for a one-click remote code execution exploit chain on a Pixel 3. (Gong's exploit received an additional $40,000 from the Chrome Rewards Program.)



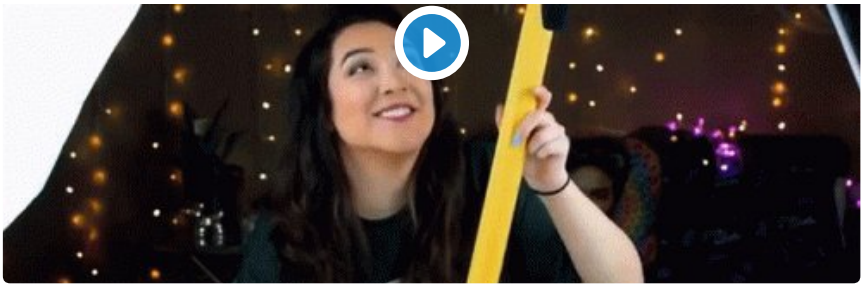
FURTHER READING
A glut of iOS 0-days pushes their price below cost of those for Android

The new rewards come almost three months after third-party exploit broker Zerodium started paying $2.5 million for zero-day attacks compromising Android, a 25-percent premium over comparable exploits for iOS. As tempting as it is to contrast the Zerodium's top Android payouts to those from Google, don't. The talent and amount of work required to develop a weaponized exploit for Zerodium are considerably higher than what Google demands, making for an apples-to-oranges comparison.

Update: Security researcher Saleem Rashid makes a good case why Google's bump in rewards is significant, and in some important ways beats out prices paid by Zerodium:

> **Saleem Rashid**
> @saleemrash1d
>
> i think we're in the midst of an iOS/Android security paradigm shift twitter.com/arstechnica/st…
>
> > **Ars Technica** @arstechnica
> > Google will pay $1.5 million for the most severe Android exploits arstechnica.com/information-te… by @dangoodin001
>
> ♡ 29 6:52 PM - Nov 21, 2019
>
> See Saleem Rashid's other Tweets

> **Saleem Rashid** @saleemrash1d · Nov 21, 2019
> Replying to @saleemrash1d
> the kicker is $500,000 for lockscreen bypass or data exfiltration, or $750,000 if it works on developer preview versions
>
> **Saleem Rashid**
> @saleemrash1d
>
> for context: Zerodium will only pay $100,000 for a lockscreen bypass on either iOS or Android.
>
> Google are offering up to 7.5(!) times as much



♡ 7 7:00 PM - Nov 21, 2019

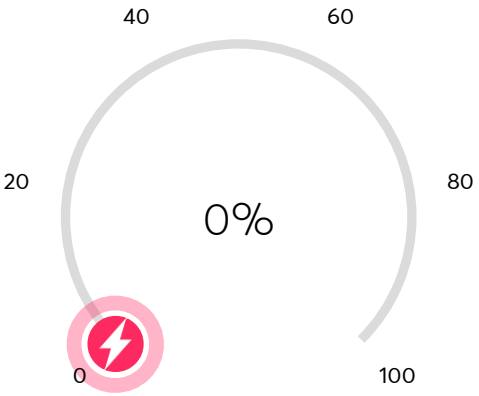
See Saleem Rashid's other Tweets

ACTION BUTTON

ars TECHNICA

What percentage of Americans say they have experienced a serious data breach?

Data breaches have resulted in millions of stolen or lost records in 2019.



Share T&Cs

READER COMMENTS 32

SHARE THIS STORY

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

CHANNEL ars

How Mind Control Saved Oddworld: Abe's Oddysee

When Lorne Lanning first conceived of what would become Oddworld, he wasn't necessarily setting out to make video games. What he needed to do was tell a story. On this episode of War Stories, we hear from the co-founder of Oddworld Inhabitants and learn all the ups and downs of Abe's journey to the screen over the past 22 years, including what comes next for the franchise in Oddworld: Soulstorm.

How Mind Control Saved Oddworld: Abe's Oddysee

Nintendo's Corey Olcsvary plays you Super Mario Maker 2 levels

Bioware answers unsolved mysteries of the Mass Effect universe

Civilization: It's good to take turns War Stories

More videos

← PREVIOUS STORY

NEXT STORY →

Related Stories

Sponsored Stories

Powered by outbrain

35 of the Most Creative and Clever Celebrity Tombstones
Direct Expose

[Pics] Forgotten For Years, This Pet Was Found In Elderlies Apartment Like This
Ice Pop

[Photos] Diver Didn't Understand What He Saw Until He Swam Closer
JOL

Discover how science is being used to create sustainable experiences
Dassault Systèmes

Future cities: "We have to act right now"
Siemens

[Photos] Why Prince Harry And Prince William's Step Sister Is Kept Out Of The Limelight
Affluent Times

Today on Ars