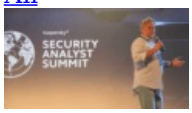
Threatpost | The first stop for security news

- Categories
  - Category List
    - Cloud Security
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Mobile Security
    - Privacy
  - Category List
    - SAS
    - Vulnerabilities
    - Web Security
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - Additional Categories
    - Slideshows
  - The Kaspersky Lab News Service
- Featured
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - The Kaspersky Lab News Service

Featured Posts

All



Security Analyst Summit 2017 Day One...

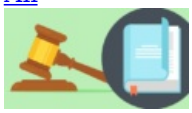

Lazarus APT Spinoff Linked to Banking...


Fileless Banking Malware Attackers Break In,...

- Podcasts

Latest Podcasts

All


Harley Geiger on Cybersecurity Policy


Threatpost News Wrap, March 27, 2017


Jon Oberheide on Perimeter Security

Threatpost News Wrap, March 17, 2017


Cody Pierce on the Future of...


Threatpost News Wrap, March 10, 2017

Recommended

The Kaspersky Lab Security News Service

- Videos

Latest Videos

All

 iOS 10 Passcode Bypass Can Access...

 BASHLITE Family Of Malware Infects 1...

 How to Leak Data From Air-Gapped...

 Bruce Schneier on the Integration of...

Chris Valasek Talks Car Hacking, IoT,...

 Patrick Wardle on OS X Malware...

Recommended

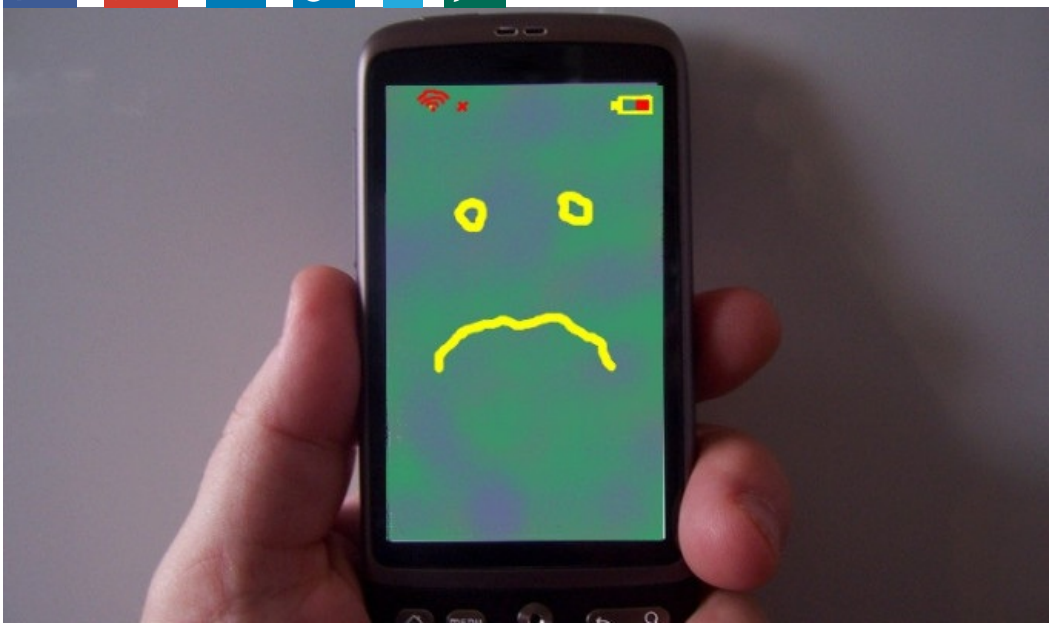
The Kaspersky Lab Security News Service

Search

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

Welcome > Blog Home>Hacks > Baseband Zero Day Exposes Millions of Mobile Phones to Attack

77 17 0 0 0



Baseband Zero Day Exposes Millions of Mobile Phones to Attack

by Tom Spring April 7, 2017 , 4:10 pm

MIAMI—A previously undisclosed baseband vulnerability impacting Huawei smartphones, laptop WWAN modules and IoT components was revealed Thursday at the Infiltrate Conference by researcher Ralf-Phillip Weinmann, managing director at security firm Comsecuris. In one attack scenario, the vulnerability could be used by attackers to execute a memory-corruption attack against vulnerable devices over the air.

Successful exploits, however, have a number of difficult requirements that reduce the overall risk to users.

Related Posts

Microsoft Quietly Kills Controversial Wi-Fi Sense Feature

May 16, 2016 , 3:31 pm

Remotely Exploitable 'Test Interface' Found in Cisco Wireless Routers

January 13, 2014 , 11:27 am

Some Netgear Routers Open to Remote Authentication Bypass, Command Injection

October 25, 2013 , 11:09 am

Weinmann said the baseband vulnerability is within the HiSilicon Balong integrated 4G LTE modems. Hisilicon Technologies is a subsidiary of Huawei Technologies. The Balong application processor is called Kirin. The flawed firmware is present in a number of high-end Huawei Honor smartphones including the P10, Huawei Mate 9, Honor 9, 7, 5c and 6, Weinmann said.

The researcher could not confirm how many of the specific models are impacted by the flaw. He estimated tens of millions of Honor smartphones could be vulnerable to attack by the chipset. He said 33 million Honor smartphones were shipped in third quarter of 2016 alone and that as many as 50 percent of the phones are likely using the HiSilicon Balong chipset.

Baseband is firmware used by cellular modem manufacturers and used on smartphones to connect to cellular networks, send and receive data, and make voice calls. Baseband vulnerabilities expose modems to a range of vulnerabilities, according to Weinmann, who has been researching baseband vulnerabilities for years.

Baseband vulnerabilities give attackers the ability to monitor a phone's communications, place calls, send premium SMS messages or cause large data transfers unbeknownst to the owner of the phone.

In his talk, Weinmann gave an overview of several baseband vulnerabilities found in the Kirin application processor, citing them as an examples of a new and vulnerable attack surface worth the security community's attention.

In addition to Huawei smartphones, an undisclosed number of laptops manufactured by a leading computer maker that use the HiSilicon Balong integrated modem are also vulnerable to attacks. The modem is also slated to be used in a number IoT and automobiles deployments, Weinmann said.

"This baseband is much easier to exploit than other basebands. Why? I'm not sure if this was intentional, but the vendor actually published the source code for the baseband which is unusual," Weinmann said. "Also, the malleability of this baseband implantation doesn't just make it good for device experimenting, but also network testing."

Weinmann suspects HiSilicon may have inadvertently released the Kirin firmware source code as part of a developer tar archive associated with the Huawei H60 Linux kernel data. Further analysis allowed him to find additional vulnerabilities within the baseband's POSIX compliant operating system.

Huawei did not return requests for comment.

In his investigation, Weinmann determined the firmware VxWorks was used, and found the command execution program C-Shell. "When I found this, I was struck by how weird this was. This allows you to call arbitrary exported functions. It's a not full shell and didn't quite allow you to do much more than toy around with things."

Despite the limited C-Shell functions, he was able to dump and modify memory, get task info, start new tasks and load dynamic kernel modules from standard input.

In his talk, Weinmann demonstrated several ways to hack phones reusing some of the IMS NIC functionality to establish cellular data connections from baseband without any visibility from the Android OS.

Since 2011, at his Black Hat presentation, Weinmann has warned of such baseband hacks. In the past, he has found bugs found in the firmware on mobile phone chipsets sold by Qualcomm and Infineon Technologies running on both iPhones and Android devices.

One attack scenario discussed is complex and involves setting up a fake base station using open-source software called OpenLTE that spoofs a network operator. He then is able to send specially crafted packets over the air that

can crash a phone via a stack buffer overflow in the LTE stack. That causes the phone to reboot and gives the attacker the ability to install a rootkit or backdoor to enable persistent access to the device.

Another attack scenario requires physical access to the phone, carrier private key pair data, and the ability to install software tools on the firmware. “It requires key material that is stored both by the carrier and on the SIM card in order to pass the mutual authentication between the phone and the network. Without this key material, a base station cannot pose as a legit network towards the device.” For this reason, in this context the vulnerability represents a low threat, he said.

Weinmann was able bring down the cost and complexity of his testing by creating his own VxWorks build environment using an evaluation version of VxWorks 7.0 that shipped with Intel Galileo several years ago. This, he said, was to have a Lua scripting interpreter run in the baseband allowing for further exploration.

Offensive testing of this technology is also risky, considering wiretapping laws that make it federal offense to illegally intercept licensed frequencies used by wireless carriers.

More specific details regarding the vulnerability are being withheld until Huawei has a chance to address and patch the vulnerability, Weinmann said. “I have chosen to only disclose lower-severity findings for now. Higher severity findings are in the pipeline.”

77 17 0 0 0

Categories: Hacks, Mobile Security, Privacy, Vulnerabilities

Leave A Comment

Your email address will not be published. Required fields are marked *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name

Email

Post Comment

reCAPTCHA

Please upgrade to a supported browser to get a reCAPTCHA challenge.

Alternatively if you think you are getting this page in error, please check your internet connection and reload.

Why is this happening to me?

Privacy - Terms

☐ Notify me of follow-up comments by email.

☐ Notify me of new posts by email.

Recommended Reads

95 10 0 585 3

May 16, 2016 , 3:31 pm
Categories: Privacy, Web Security

Microsoft Quietly Kills Controversial Wi-Fi Sense Feature

by Tom Spring

Later this summer, when Microsoft rolls out a massive update to Windows 10 called Anniversary Edition, notably missing will be the controversial Wi-Fi Sense feature.

Read more…

0 0 0 0 0

January 13, 2014 , 11:27 am
Categories: Vulnerabilities, Web Security

Remotely Exploitable 'Test Interface' Found in Cisco Wireless Routers

by Dennis Fisher

There is a serious vulnerability in several Cisco wireless routers that could give an attacker root level access. The bug is the result of a backdoor in the routers that was set up as a test interface, and Cisco does not yet have patches available to fix it.

Read more…

0 0 0 0 1

October 25, 2013 , 11:09 am
Categories: Vulnerabilities, Web Security

Some Netgear Routers Open to Remote Authentication Bypass, Command Injection

by Dennis Fisher

There is a vulnerability in some Netgear wireless routers that allows a remote attacker to

Read more…

Top Stories

Creating a More Altruistic Bug Bounty Program

April 7, 2017 , 2:22 pm

No Firewalls, No Problem for Google

February 15, 2017 , 7:00 am

Lines Around Cyber Threat Intelligence Sharing Blurring

April 3, 2017 , 2:00 pm

Apache Struts 2 Exploits Installing Cerber Ransomware

April 7, 2017 , 12:46 pm

Google, Jigsaw Partner on Free Tools to Secure Elections

March 22, 2017 , 3:38 pm

Memory Corruption Mitigations Doing Their Job

April 3, 2017 , 1:00 pm

Threatpost News Wrap, March 31, 2017

March 31, 2017 , 11:55 am

Telepresence Robots Patched Against Data Leaks

March 13, 2017 , 11:59 am

The Final Say

From Kaspersky Blogs

From Southernmost City to Southernmost Continent….

Hi folks! It’s been a while, I know. However, I’ve a fairly good excuse: Antarctic comms leave a lot to be desired, and it’s there where I’ve been the last ~two weeks!… Q…

Read more…

Ransomware in targeted attacks…

Ransomware's popularity has attracted the attention of cybercriminal gangs; they use these malicious programs in targeted attacks on large organizations in order to steal money. In late 2016, we detec…

Read more…

Protected: Risking data heartache: it hurts to los…

There is no excerpt because this is a protected post.…

Read more…

Eight targeted ransomware attacks aiming for your …

Our experts have identified at least eight independent threat actors competing for the right to extort money from businesses.…

Read more…

Kaspersky Academy attended MIT (IC)3 Annual Confer...

72 guests, among them a global security lead Gordon Morrison, attended the MIT (IC)3 Annual Conference to share the latest insights into the industry. Educational programs manager Christel Gampig-Avil…

Read more...

Threatpost | The first stop for security news The Kaspersky Lab Security News Service
Categories Black Hat | Cloud Security | Critical Infrastructure | Cryptography | Featured | Government | Hacks | IoT | Malware | Mobile Security | Podcasts | Privacy | Security Analyst Summit | Slideshow | Uncategorized | Videos | Vulnerabilities | Web Security

- RSS Feeds
- Home
- About Us
- Contact Us

Authors

Michael Mimoso
Tom Spring
Christopher Brook

Copyright © 2017 Threatpost | The first stop for security news

- | Terms of Service
- | Privacy