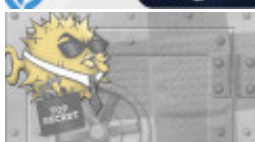


Threatpost | The first stop for security news

- [Categories](#)
 - [Category List](#)
 - [Apple](#)
 - [Cloud Security](#)
 - [Compliance](#)
 - [Critical Infrastructure](#)
 - [Cryptography](#)
 - [Government](#)
 - [Category List](#)
 - [Hacks](#)
 - [Malware](#)
 - [Microsoft](#)
 - [Mobile Security](#)
 - [Privacy](#)
 - [Ransomware](#)
 - [Category List](#)
 - [SAS](#)
 - [SMB Security](#)
 - [Social Engineering](#)
 - [Virtualization](#)
 - [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](#)[Apple's 'Targeted' Gatekeeper Bypass Patch Leaves...](#)[Morale Remains Low Around Health and...](#)[OpenSSH Patches Critical Flaw That Could...](#)

- [Podcasts](#)

Latest Podcasts

[All](#)



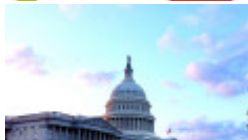
[Threatpost News Wrap, January 15, 2016](#)



[Threatpost News Wrap, January 8, 2016](#)



[Threatpost's 2015 Year in Review](#)



[Threatpost News Wrap, October 30, 2015](#)



[Gary McGraw on BSIMM6 and Software...](#)



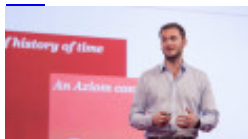
[Threatpost News Wrap, October 23, 2015](#)

Recommended

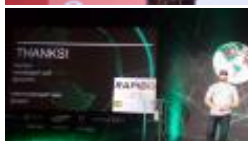
- [The Kaspersky Lab Security News Service Videos](#)

Latest Videos

[All](#)



[Kris McConkey on Hacker OpSec Failures](#)



[Trey Ford on Mapping the Internet...](#)



[Christofer Hoff on Mixed Martial Arts,...](#)



[Twitter Security and Privacy Settings You...](#)



[The Biggest Security Stories of 2013](#)



[Jeff Forristal on the Android Master-Key...](#)

Recommended

[The Kaspersky Lab Security News Service](#)

- [Twitter](#)
- [Facebook](#)
- [Google](#)
- [LinkedIn](#)
- [YouTube](#)
- [RSS](#)



[Welcome](#) > [Blog Home](#) > [Vulnerabilities](#) > Serious Linux Kernel Vulnerability Patched



Serious Linux Kernel Vulnerability Patched

[Follow @mike_mimoso](#) by [Michael Mimoso](#) January 19, 2016 , 7:47 am

A patch for a critical Linux kernel flaw, present in the code since 2012, is expected to be pushed out today.

The vulnerability affects versions 3.8 and higher, said researchers at startup Perception Point who discovered the vulnerability. The flaw also extends to two-thirds of Android devices, the company added.

Related Posts

[OpenSSH Patches Critical Flaw That Could Leak Private Crypto Keys](#)

January 14, 2016 , 2:33 pm

[Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47](#)

December 2, 2015 , 11:18 am

[Lenovo Patches Vulnerabilities in System Update Service](#)

November 25, 2015 , 10:00 am

“It’ s pretty bad because a user with legitimate or lower privileges can gain root access and compromise the whole machine,” Yevgeny Pats, cofounder and CEO of Perception Point. “With no auto update for the kernel, these versions could be vulnerable for a long time. Every Linux server needs to be patched as soon the patch is out.”

Pats said an attacker would require local access to exploit the vulnerability on a Linux server. A malicious mobile app would get the job done on an Android device (Kit-Kat and higher), he said. Pats added that exploitation of the flaw is fairly straightforward, but it’ s unknown whether it’ s been attacked to date.

“The fix was simple,” Pats said. “The problem is not all devices Linux get patched automatically.”

The vulnerability, CVE-2016-0728, lives in the keyring facility built into the various flavors of Linux. The keyring encrypts and stores login information, encryption keys and certificates, and makes them available to applications. In a report published by Perception Point, researchers said the vulnerability is a [reference leak](#) that can be abused to ultimately execute code in the Linux kernel.

“User space applications give [keyring] the option to manage the crypto keys,” Pats said. “The user doesn’ t have to manage keys; the OS does it for the application. Apps use it for security reasons. When they want to apps to work with crypto, they use this feature. The feature has kernel access; the OS gives the userland app the ability to use this feature. The problem is that the code runs in the kernel.”

Pats said that SMEP (Supervisor Mode Execution Protection) and SMAP (Supervisor Mode Access Protection) make exploitation difficult on Linux servers, while SELinux does the same for Android devices. SMEP and SMAP are relatively new features that prevent the kernel from accessing and executing code from userland.

The flaw may linger a little longer on Android devices, since most updates are not pushed automatically by carriers and manufacturers. Android is built upon the Linux kernel, but customized without many of the libraries that accompany standard Linux builds.

Perception Point published a technical analysis of the vulnerability and how to exploit it, including [proof-of-concept code](#) published to its Github page.



Categories: [Vulnerabilities](#), [Web Security](#)

Leave A Comment


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

Comment

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

Name Email

☐ I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

- ☐ Notify me of follow-up comments by email.
- ☐ Notify me of new posts by email.

Recommended Reads



163



321



296



0



0

January 14, 2016 , 2:33 pm

Categories: [Cryptography](#), [Featured](#), [Vulnerabilities](#)

[OpenSSH Patches Critical Flaw That Could Leak Private Crypto Keys](#)

by [Michael Mimoso](#)

OpenSSH patched a critical vulnerability that could be exploited by an attacker to force a client to leak private cryptographic keys.

[Read more...](#)



December 2, 2015 , 11:18 am

Categories: [Vulnerabilities](#), [Web Security](#)

[Google Ends Chrome Support on 32-bit Linux. Releases Chrome 47](#)

by [Chris Brook](#)

Google released Chrome 47 this week and announced that it will end Chrome support for older, 32-bit Linux distributions early next year.

[Read more...](#)



November 25, 2015 , 10:00 am

Categories: [Hacks](#), [Vulnerabilities](#)

[Lenovo Patches Vulnerabilities in System Update Service](#)

by [Michael Mimoso](#)

Lenovo has patched two serious vulnerabilities in Lenovo System Update that can allow hackers elevate privileges and guess admin passwords.

[Read more...](#)

Top Stories

[Serious Linux Kernel Vulnerability Patched](#)

January 19, 2016 , 7:47 am

[SLOTH Attacks Up Ante on SHA-1, MD5 Deprecation](#)

January 7, 2016 , 10:50 am

[Google Patches Critical Android Mediaserver Vulnerability](#)

December 8, 2015 , 11:21 am

[OpenSSH Patches Critical Flaw That Could Leak Private Crypto Keys](#)

January 14, 2016 , 2:33 pm

[Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47](#)

December 2, 2015 , 11:18 am

[Questions Linger as Juniper Removes Backdoored Dual_EC RNG](#)

January 11, 2016 , 4:48 pm

[New JavaScript Ransomware Sold as a Service](#)

January 4, 2016 , 11:04 am

[Denial-of-Service Flaw Patched in DHCP](#)

January 13, 2016 , 10:00 am

[Mozilla Warns of SHA-1 Deprecation Side Effects](#)

January 7, 2016 , 2:04 pm

TIP #3



**Security policies
should work
everywhere**

even outside the workplace

[Click to learn more](#)

The Final Say

From Kaspersky Blogs



[Bucking Barranco!...](#)

Climbing the Barranco lava wall of Kilimanjaro was by far the highlight of our week-long ascent up Africa's tallest volcano – that is, after the final leg up to the summit via Stella Artois Poin...

[Read more...](#)



[Targeted Mobile Implants in the Age of Cyber-Espio...](#)

Despite a strong data encryption, a compromised mobile end point is completely exposed to spying, since threat actors have the same ability to read messages as users themselves. Threat actors don't ne...

[Read more...](#)



[SIM cards: attack of the clones](#)

SIM cards can be cloned. How is it possible and what does it have to do with cybercriminals?

[Read more...](#)



[Cyberincidents responsibility: The poll](#)

Should employees' cybersecurity awareness be tested by HR?

[Read more...](#)



[Five minutes with Alexander Erofeev...](#)

We are continuing series of the interviews with Kaspersky Lab experts enquiring their opinion regarding cyber-security industry and related threats. Today, Alexander Erofeev, Chief Marketing Officer a...

[Read more...](#)

[Threatpost](#) | [The first stop for security news](#) The Kaspersky Lab Security News Service
[Categories](#) [Apple](#) | [Black Hat](#) | [Cloud Security](#) | [Compliance](#) | [Critical Infrastructure](#) |
[Cryptography](#) | [Data Breaches](#) | [Featured](#) | [Google](#) | [Government](#) | [Hacks](#) | [How I Got](#)
[Here](#) | [Malware](#) | [Microsoft](#) | [Mobile Security](#) | [Podcasts](#) | [Privacy](#) | [Ransomware](#) |
[Scams](#) | [Security Analyst Summit](#) | [Slideshow](#) | [SMB Security](#) | [Social Engineering](#) |
[Uncategorized](#) | [Videos](#) | [Virtualization](#) | [Vulnerabilities](#) | [Web Security](#)

- [RSS Feeds](#)
- [Home](#)
- [About Us](#)
- [Contact Us](#)

Authors

[Michael Mimoso](#)
[Christopher Brook](#)

Copyright © 2016 [Threatpost](#) | [The first stop for security news](#)

- | [Terms of Service](#)
- | [Privacy](#)

