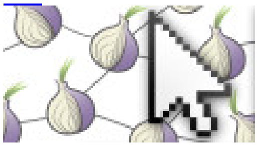
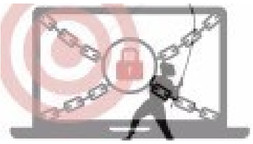
Threatpost | The first stop for security news

- 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


Tor Project to Launch Bug Bounty…


New JavaScript Ransomware Sold as a…

Six Things to Watch for in…

- Podcasts

Latest Podcasts

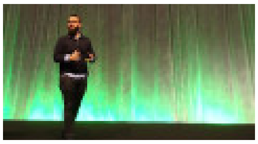
All

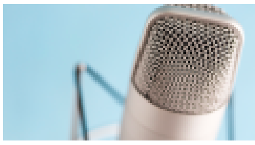
[Threatpost’ s 2015 Year in Review]

[Threatpost News Wrap, October 30, 2015]

[Gary McGraw on BSIMM6 and Software…]

[Threatpost News Wrap, October 23, 2015]

 [Juan Andres Guerrero-Saade on the Dangers…]

 [Threatpost News Wrap, October 16, 2015]

Recommended

- Robert Hansen on Aviator, Search Revenue and the $250,000 Security Guarantee
- Threatpost News Wrap, February 21, 2014
- How I Got Here: Jeremiah Grossman
- Chris Soghoian on the NSA Surveillance and Government Hacking

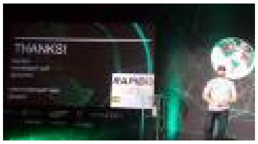
The Kaspersky Lab Security News Service

- Videos

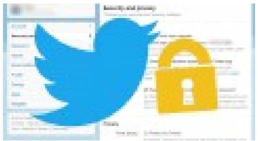
Latest Videos

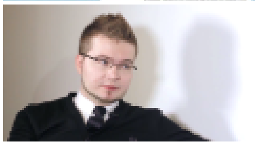
All

[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

- Twitter Security and Privacy Settings You Need to Know
- Lock Screen Bypass Flaw Found in Samsung Androids
- Facebook Patches OAuth Authentication Vulnerability
- Video: Locking Down iOS

The Kaspersky Lab Security News Service

Search

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

- 🇬🇧
- 🇷🇺

Welcome > Blog Home>Web Security > Zerodium Offers $100K for Adobe Flash Heap Isolation Bypasses

19 21 24 0 0

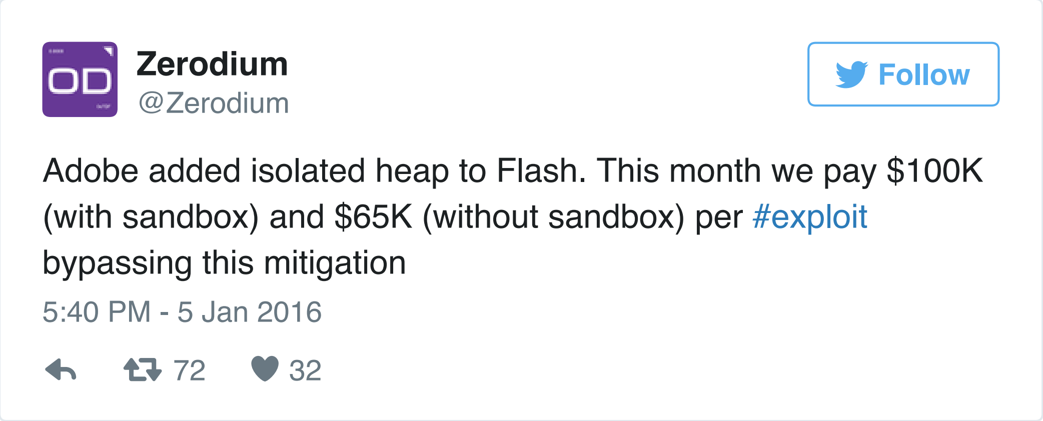
Zerodium Offers $100K for Adobe Flash Heap Isolation Bypasses

Follow @mike_mimoso by Michael Mimoso January 5, 2016 , 1:55 pm

Despite calls to eliminate Adobe Flash Player, researchers inside and outside the vendor continue to invest in and build mitigations against modern attacks.

As recently as three weeks ago, Adobe announced it had rewritten its memory manager, laying the groundwork for widespread heap isolation, which is an important protection against use-after-free vulnerability exploits.

Today, however, exploit acquisition company Zerodium announced via its Twitter account that it would run a month long bounty program, paying as much as $100,000 for exploit code bypassing the heap isolation mitigation in Flash Player.



Zerodium
@Zerodium

Follow

Adobe added isolated heap to Flash. This month we pay $100K (with sandbox) and $65K (without sandbox) per #exploit bypassing this mitigation

5:40 PM - 5 Jan 2016

72 32

Zerodium, launched in July by VUPEN founder Chaouki Bekrar, buys high-risk zero-day vulnerabilities for all major platforms and third-party applications. Bekrar said that the attacks his company purchases would be available to customers via a feed of vulnerabilities, exploits and defensive capabilities; none of the attacks would be made public.

In September, the controversial Bekrar announced that Zerodium would host a million-dollar bounty for browser-based and untethered jailbreaks for Apple iOS 9, which had just been released. Zerodium announced at the end of the bounty that there was one winning team, but no details were released about the winners or the exploit. In November, the company published payouts for eligible zero-days.

Zerodium’ s bounty is just the latest assault against Adobe Flash Player, which has been the focus of a number of high-profile targeted nation-state attacks, as well as a favorite target of exploit kits used to great profit by cybercrime outfits.

Many in the security community have pleaded with organizations to ban the use of Flash Player because of its history of vulnerabilities. Adobe, for its part, pushes out what has become almost a scheduled monthly security update for Flash; the December update alone was a massive release that addressed 79 vulnerabilities, most of those enabling memory-based attacks such as use-after-free.

Use-after-free attacks have been a favorite vector for attackers, who have steadily gravitated away from buffer over exploits and in this direction. Adobe has received help from its partners in addressing this problem, with Google’ s Project Zero research team the highest-profile participant.

In July, Project Zero introduced heap partitioning, which was integrated into Flash Player; the technique isolates different types of objects on the heap, Google said, adding that Chrome and other browsers make extensive use of this technique.

Prior to using Heap isolation, Adobe used a single heap for ActionScript objects, giving an attacker the luxury of attacking a Vector object and dictating where objects are allocated. By corrupting memory in this way, attackers could read and write in virtual memory and bypass ASLR to execute code. Heap isolation prevents this by allocating Vector objects in a separate heap, eliminating the attacker’ s ability to corrupt memory in this way. The technique isn’ t foolproof, however, as Endgame Systems proved when in November it published a bypass for heap isolation in Flash.

Heap isolation isn' t the only new mitigation to find its way into Flash in the last 12 months. Adobe said in December that it worked with Microsoft as an early adopter of its Control Flow Guard to protect static and dynamic code in Flash Player.

19 21 24 0 0

Categories: Web Security, 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

□ I'm not a robot

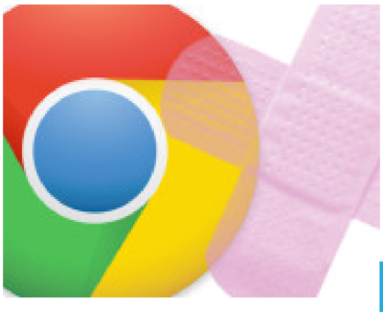
reCAPTCHA
Privacy - Terms

Post Comment

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

Recommended Reads



53 311 39 0 0

December 9, 2015 , 9:22 am
Categories: Web Security, Vulnerabilities, Google

Google Updates Chrome, Extends Safe Browsing to Chrome for Android

by Michael Mimoso

Google joined the Patch Tuesday parade with a Chrome update that patches seven vulnerabilities in the browser. It also announced it was extending Safe Browsing protection to Chrome for Android.

Read more...

121 331 198 0 0

December 3, 2015 , 8:00 am
Categories: Web Security, Vulnerabilities

Flash’ s Farewell Under Way

by Michael Mimoso

Adobe’ s announcement that it has retooled—and renamed—Flash is a longterm signal that the vulnerable and fatigued platform is on its last legs.

Read more...

34 71 47 0 0

November 12, 2015 , 1:33 pm
Categories: Vulnerabilities

Exploit Writing and Mitigation Going Hand in Hand

by Michael Mimoso

Researchers at Endgame shared how two exploit mitigations could go a long way toward wiping out a nasty class of vulnerabilities.

Read more...

Top Stories

Zerodium Offers $100K for Adobe Flash Heap Isolation Bypasses

January 5, 2016 , 1:55 pm

VMware Patches Pesky XXE Bug in Flex BlazeDS

November 20, 2015 , 4:36 pm

Google Patches Critical Android Mediaserver Vulnerability

December 8, 2015 , 11:21 am

ProtonMail Back Online Following Six-Day DDoS Attack

November 9, 2015 , 1:00 pm

Google Ends Chrome Support on 32-bit Linux, Releases Chrome 47

December 2, 2015 , 11:18 am

Microsoft Patches Denial of Service Issue in Hyper-V

November 12, 2015 , 11:39 am

Exploit Writing and Mitigation Going Hand in Hand

November 12, 2015 , 1:33 pm

High-Risk SAP HANA Vulnerabilities Patched

November 9, 2015 , 12:13 pm

Patched Libpng Vulnerabilities Have Limited Scope

November 17, 2015 , 1:12 pm

TIP #3
Security policies should work everywhere
even outside the workplace
Click to learn more

The Final Say

From Kaspersky Blogs

Around the world in 2015....

Everything about New Year is good! And one of the best things is that it’ s the perfect time to take a break, take stock, take note, share impressions, and recharge the batteries for next year. I...

Read more…

Social Networks – A Bonanza for Cybercriminals...

Security experts have for years reiterated: cybercriminals can make use of any information that you publish about yourself on a social network. However, a huge amount of users still continue to share ...

Read more…

The evolution of the SIM card

Observing the evolution the good old SIM card went through and the results so far

Read more…

A few recommendations on the cybersecurity of the ...

For the first 2016 Kaspersky Business blog post, we've chosen Commandments of Office Security, a handful of common problems with cybersecurity in the workplace, and the ways to solve - or at least mit...

Read more…

Are fitness trackers dangerous?...

One of the most popular gadgets today (if we don’ t include smartphones and tablets, of course) is the fitness tracker – usually in the form of a bracelet or wrist watch. This small device is so ...

Read more…

Threatpost | The first stop for security news The Kaspersky Lab Security News Service CategoriesApple | Black Hat | Cloud Security | Compliance | Critical Infrastructure | Cryptography | Data Breaches | Featured | Featured Podcast | Featured Video | 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

- | Terms of Service
- | Privacy