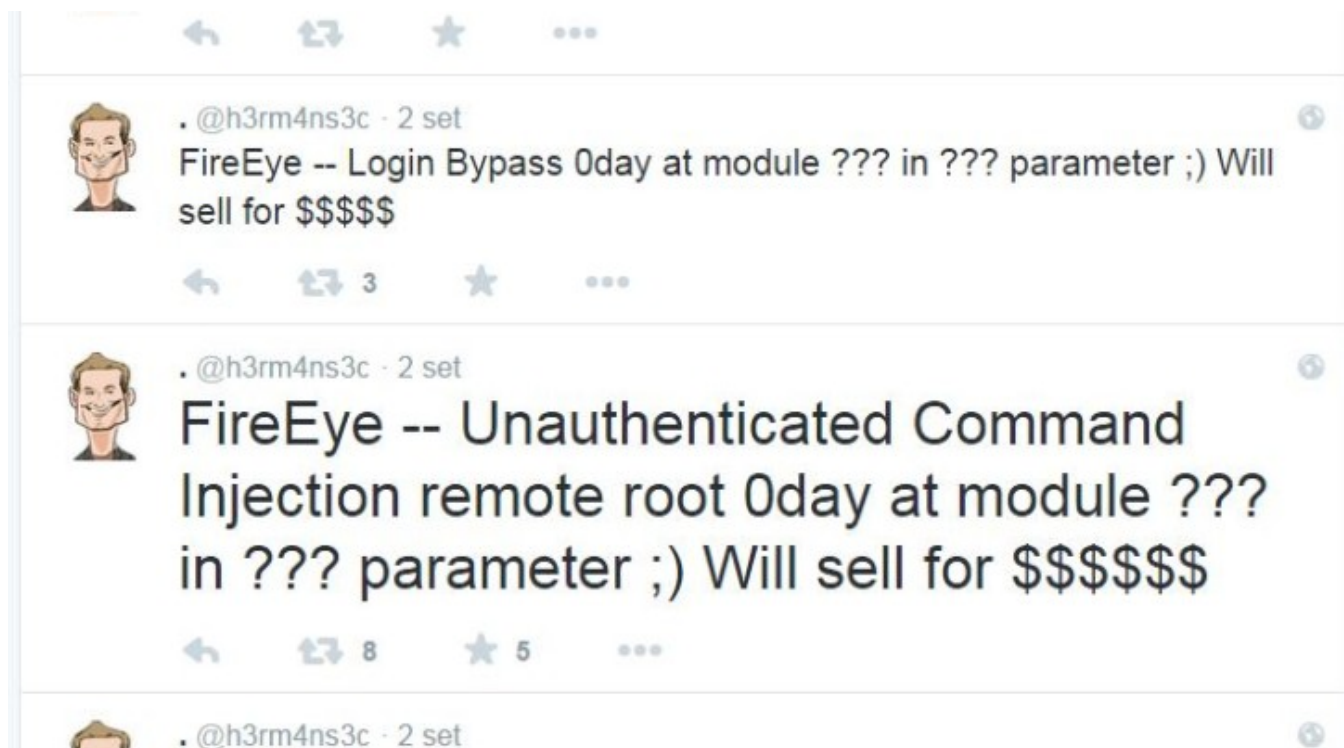


**MUST READ** Fiat Chrysler recalls thousands Jeep Renegade SUVs due to hacking risks

## Researcher disclosed 0day flaw in FireEye and offers others for sale

September 7, 2015 By [Pierluigi Paganini](#)



The expert Kristian Erik Hermansen disclosed a zero-day flaw in the FireEye core appliance that could be exploited to gain remote root file system access.

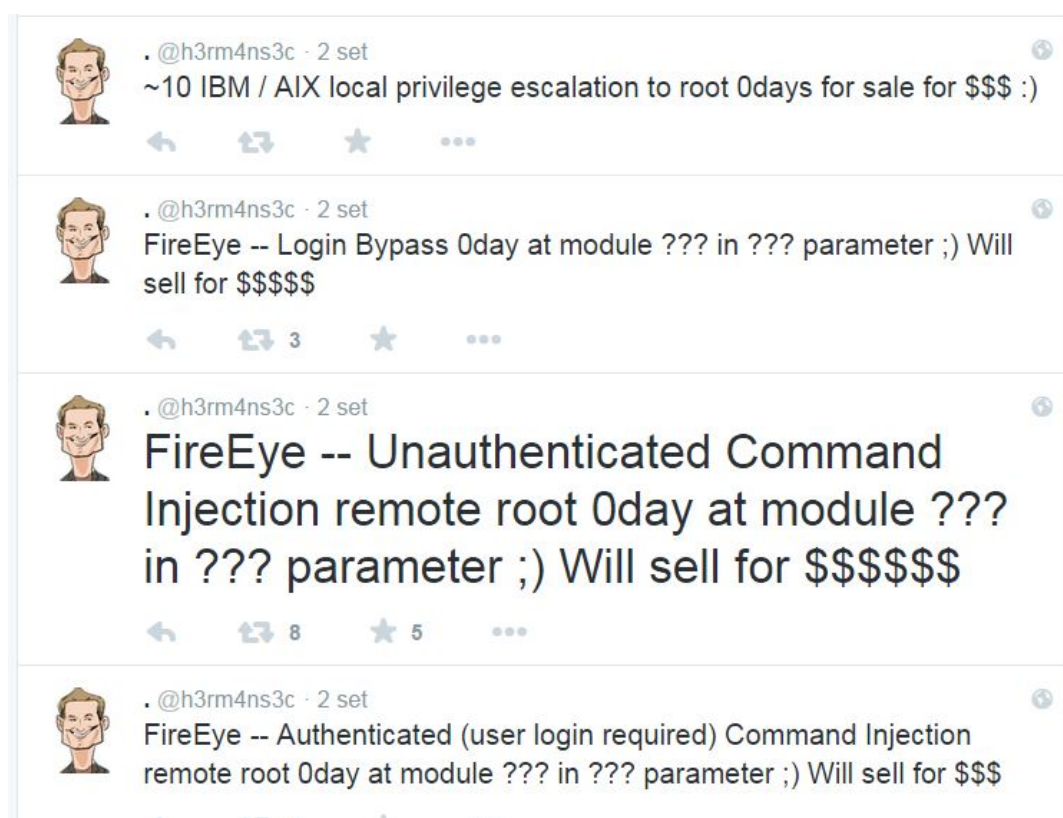
Yesterday security researcher [Kristian Erik Hermansen](#) disclosed a zero-day vulnerability in the

FireEye core appliance that could be exploited to gain remote root file system access.

Hermansen told to [CSOonline](#) that he was working with the colleague Ron Perris when discovered thirty vulnerabilities in FireEye's product, including multiple remote root issues.

The expert also published a proof of concept to show how to trigger the vulnerability to copy the /etc/passwd file.

Here starts the bad news for FireEye because Hermansen claims to have discovered other three zero-day and is offering them for sale. Hermansen claims to have found a login bypass vulnerability, a command injection vulnerabilities.



The disclosed flaw seems to affect a PHP script on the FireEye appliance, the expert has publicly criticized the implementation of the popular security firm.

“

*“FireEye appliance, unauthorized remote root file system access. Oh cool, web server runs as root! Now that’s excellent security from a \_security\_ vendor 😊 Why would you trust these people to have this device on your network,” wrote Hermansen in a note.*

*“Just one of many handfults of FireEye / Mandiant 0day. Been sitting on this for more than 18 months with no fix from those security “experts” at FireEye. Pretty sure Mandiant staff coded this and other bugs into the products. Even more sad, FireEye has no external security researcher reporting process.”*

Hermansen posted the PoC for the FireEye remote root file system access 0-day on [Pastebin](#), he is offering the other vulnerabilities for sale and the base asking price starts at around \$10,000 USD per bug.

“

*“I tried for 18 months to work with FireEye through responsible channels and they balked every time. These issues need to be released because the platforms are wrought with vulnerabilities and the community needs to know, especially since these are Gov-approved Safe Harbor devices with glaring remote root vulnerabilities,” Hermansen told Salted Hash via email.*

*“No one should be trusting these devices on*

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence | **elligence** **Laws**

Laws and regulations | Malware | Mobile | Security | Social Networks | Reports |

SA Team | **EXTENDED COOKIE POLICY** | Contact me |

**VED COOKIE POLIC**

Hermansen made headlines after he disclosed a number of security issues with the Covered California website as [reported](#) by Forbes:

*“Hermansen discovered a vulnerability that would allow someone to take over another person’s*

account on the California site, and review or change the information entered there. He tried contacting Covered California “at least 15 times” by email, phone or chat about the problem, but got no response for over a month. “They must have been overwhelmed by people seeking help with the site,” he said.”

Stay Tuned ...

Pierluigi Paganini

(Security Affairs – FireEye, hacking)

Share it please ...



Share this:

 Email


 Twitter 22


 Print

 LinkedIn 17

 Facebook 13

 More

 [FireEye](#) [Hacking](#) [Kristian Erik Hermansen](#) [security](#) [zero-Day](#)

 [Breaking News](#) [Hacking](#) [Security](#)

SHARE ON





Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish. [Accept](#) [Read More](#)

over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

MORE S



Stealing wireless  
The CERT wireless  
multiple download



## PREVIOUS ARTICLE

[Stealing all files from Seagate wireless disks is too easy](#)

## YOU MIGHT ALSO LIKE

[Stealing all files from Seagate wireless disks is too easy](#)

September 7, 2015 By [Pierluigi Paganini](#)

[Fiat Chrysler recalls thousands Jeep Renegade SUVs due to hacking risks](#)

September 7, 2015 By [Pierluigi Paganini](#)

[Promote your solution on Security Affairs](#)



Copyright Security Affairs by Pierluigi Paganini - All Right Reserved.

u