European credit card payment terminals are plagued with serious flaws

December 27, 2015 By Pierluigi Paganini

Two German security experts have exposed a number of serious flaws in credit card payment systems that put users at risk.

The duo of German security experts, Karsten Nohl and Fabian Braunlein, found a new vulnerability in payment terminals that could be exploited by hackers to steal money. Differently from past attacks, this time, the hackers are targeting the protocol putting billions of customers at risk.
"Previous attacks exploit software bugs, like you would have on your computer. Ones that can be fixed with a software update,"

The experts discovered a set of vulnerabilities with payment terminals used in Europe that could allow hackers to steal the victim's PIN code and magnetic strip from their card.

The experts tested payment terminals from five different payment processors that provide terminals to merchants, the systems tested used two different networks, both of which used the same back-end software.

“This is the only software used in Germany for this purpose, so everybody should be equally affected,” Nohl said.

The vulnerabilities could be exploited to force any terminal to send funds to any bank account in Germany, but the experts speculate that the flaw could affect systems in other European countries.

“Nohl and Bräunlein will lay out several different attacks, and they hinge on problems with two protocols that payment terminals use: ZVT and Poseidon. Protocols are essentially different languages that devices use to communicate.*” **reported** MotherBoard.*

The hack works wirelessly, the attacker only needs to be connected to the same wireless network.

*“The companies responsible for these security vulnerabilities, including the banks – they certainly acknowledged the issue, but they are reluctant to react to it. They’re saying – ‘fraud is not happening yet’, but it’s just a matter of time. So, by not reacting now that it’s known – they’re adding insult to injury.” **explained** the popular German code-breaker Karsten Nohl of Security Research Labs in Berlin. “Now, what we’re attacking is the protocol itself. The devices work exactly as intended and are still vulnerable. So this is a risk that cannot easily be fixed with a patch.” “The entire system would have to be overhauled,”*

Nohl explained that an attacker could trick victims into check their accounts charged for refunds that never took place in order to trigger the vulnerability. The vulnerability could be also used to clone credit card.

"Basically anything with a magnet strip and a PIN number is vulnerable to this," Nohl said "This is the first time we've come across such a large deployment, with such serious issues, and don't have an obvious fix."

According to Karsten Nohl, a criminal organization could probably reproduce the attacks "within a couple of months."

"The security of the PIN number is not quite as high as one wanted to believe, hence every system relying on the PIN is less secure than previously thought," Nohl added.

The two experts have conducted several studies in the past warning about security issues affecting the SIM cards. Two years ago Karsten Nohl revealed to The New York Times that he identified a vulnerability in encryption technology used for SIM that could allow an attacker to obtain the 56-digit SIM card's digital key necessary for the card modification. Roughly 750 million mobile phones were open to cyber attack.

Which is the response of the German banking organisation Deutsche Kreditwirtschaft?

According to Tagesschau, German banking organisation Deutsche Kreditwirtschaft who has analyzed the results of the study conducted by the experts, the system is secure. The organization claimed that the attack proposed by the experts only works under specific conditions. The Electronic commerce organisation BECN is also evaluating the results of the tests.

Pierluigi Paganini

(Security Affairs – credit card, hacking)

Hacking fraud banking credit card payment systems

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 Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with 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”.

PREVIOUS ARTICLE
InterApp, the device that can hack any Smartphone

NEXT ARTICLE
The Ramnit Botnet is back after the law enforcement takedown

YOU MIGHT ALSO LIKE

Turkish hackers took over a Russian Govt Instagram account

January 3, 2016 By Pierluigi Paganini

@FFD8FFDB Twitter bot spies on

poorly configured cameras

January 3, 2016 By Pierluigi Paganini

- +Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security) Threat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine".

Back to top