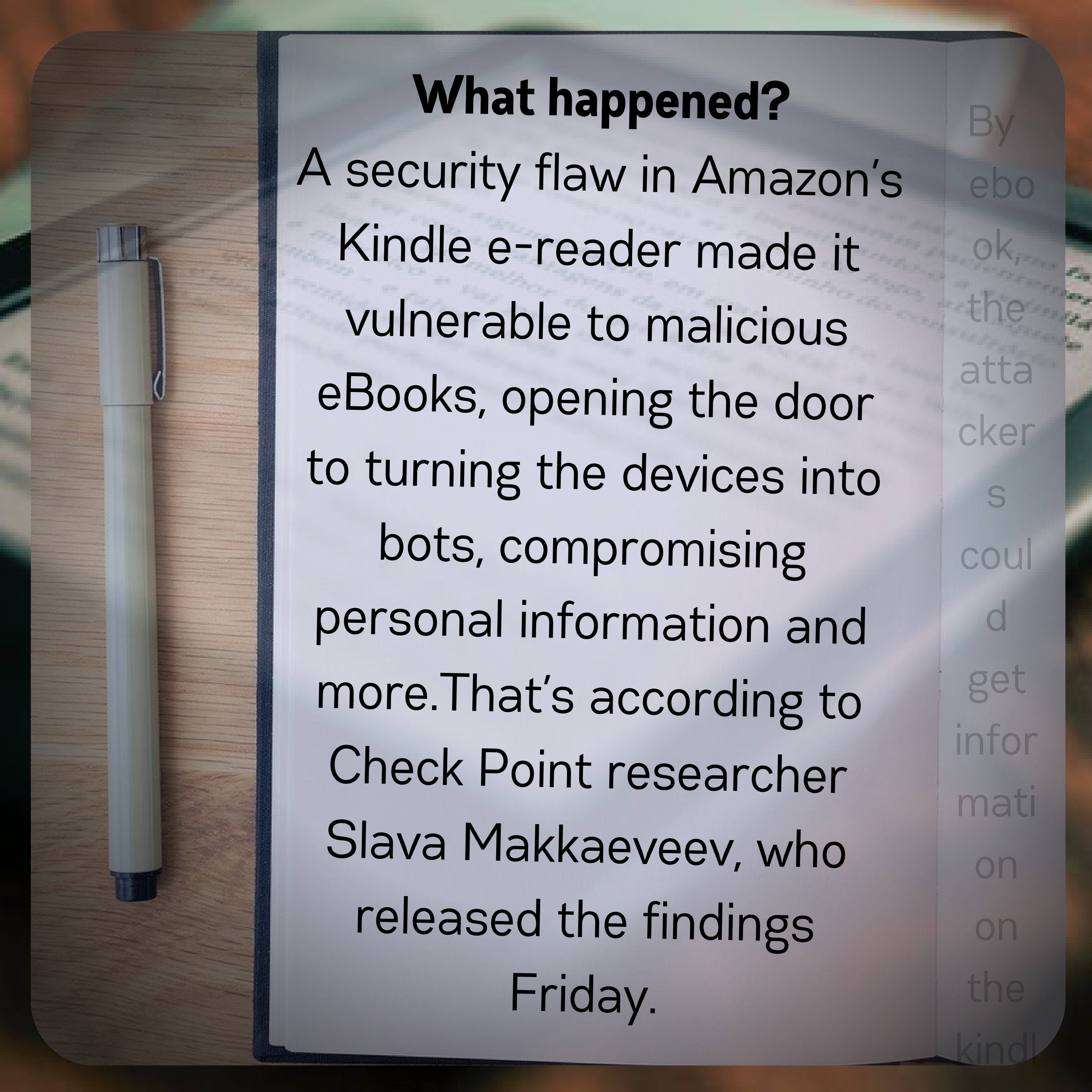
Security flaw in Amazon's Kindle e-reader

-

A CRISIS AVERTED!

OWASP
Open Web Application
Security Project



What happened?

A security flaw in Amazon's Kindle e-reader made it vulnerable to malicious eBooks, opening the door to turning the devices into bots, compromising personal information and more.That's according to Check Point researcher Slava Makkaeveev, who released the findings Friday.

By ebook, the attackers could get information on the kindl

More insights:

By sending a single malicious ebook, the attackers could get their hands on all the information on the kindle, along with the Amazon linked billing information.

If a victim clicked on the malicious eBook, it connects to a remote server and locks the user's screen.

Once access is gained, the kindle can be used as a machine to target the other devices such as mobile phones, computers etc in the household.

e
boo
the
atta
cker
s
coul
d
get
info
rma
tion
on
the

What was the bug?

The attackers exploited the implementation associated with how PDF documents are opened, by executing a malicious payload.

A heap overflow vulnerability in the PDF rendering function was exploited (CVE-2021-30354)

A local privilege escalation flaw was also exploited (CVE-2021-30355)

Is it ok now?

It's unclear if the bug was exploited prior to the patch, but crisis appears to have been averted. Any serious attack could have affected tens of millions of Kindle users across the globe.