Borns IT- und Windows-Blog
Insights & Tipps zu Windows, Linux,
Android, Tablet PCs & Co.

Backdoor in Chinese routers (Jetstream, Wavelink, Ematic)

Posted on November 24, 2020 by Günter Born

[German] A security researcher has come across a hidden back door that is built into Chinese routers from various companies (Wavlink, Jetstream). Not only can the router be controlled via the backdoor, but it can also penetrate the network of the device owner behind it. The devices are sold on Amazon, eBay and other platforms as well as at the US retailer Walmart. I don't know how much the routers are being sold in Germany. A quick search on Amazon for Ematic routers (or other device names) brought me hits.

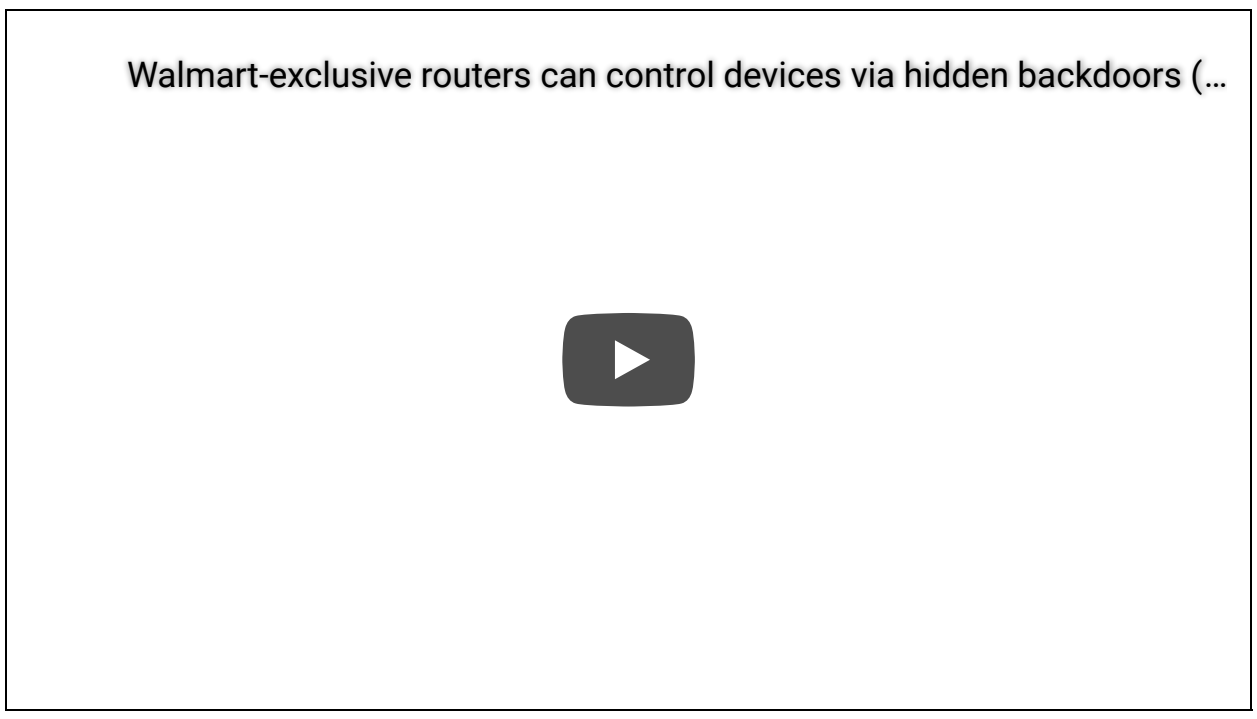
Do we need something like a German purity law for routers like: 'I only allow routers from AVM into my four walls'? If I scan the random articles from the blog that I linked to at the bottom of the post, the answer is yes. And you should patch the stuff, absolutely and regularly.

Oh, that's a backdoor in the router

A collaboration between CyberNews Sr.'s information security researcher Mantas Sasnauskas and researchers James Clee and Roni Carta discovered suspicious backdoors in a Chinese-made Jetstream router that is sold exclusively at Walmart as an "affordable" WiFi router. This back door would allow an attacker to remotely control not only the routers but also all devices connected to this network. The firmware in question is also used in other routers.

> *When asked by CyberNews, Walmart replied that they were investigating the problem, but currently had no more devices in stock and did not plan to include the device again in their range. The previous buyers are the stupid ones.*

I became through this Cybernews article aware of the topic . The following video deals with the whole thing in various details.



(What: YouTube)

In addition to the Walmart-exclusive Jetstream router, security researchers discovered that inexpensive Wavlink routers, which are usually sold on Amazon or eBay, have similar back doors. The Wavlink routers also contain a

script that lists nearby WLANs and offers the option to connect to these networks. I then took a look at Amazon - a WAVLINK AC3200 dual-band WiFi router is also offered via a sponsored link. So it cannot be ruled out that such routers - possibly under the trade name Ematic (from Media Markt I only found a streaming box under this name) - are used in Germany, Austria or Switzerland.

The security researchers have found indications that these backdoors are being actively exploited. An attempt was made to add the devices to a Mirai botnet. In Mirai is malware , the devices connected to a network infected, they transformed as part of a botnet in remote-controlled bots and used for large-scale attacks.

To the background

Originally, the security researcher Clee just had the idea of looking up the security of inexpensive Chinese devices such as Wavlink routers. He is quoted as saying, "I was interested to see how much effort companies put into security. I decided it would be a nice hobby to buy cheap Chinese technology from Amazon and see what I find out could. "

Then he contacted Carta and Sasnauskas through CyberNews. "After talking to James about his discovery," Carta told CyberNews, "I immediately tried looking for other companies using the same firmware and found that Jetstream's devices were also vulnerable. The research was interesting to understand where the vulnerability came from and how a malicious actor could fully exploit it. "

Although Jetstream has an exclusive deal with Walmart and is sold under other brand names such as Ematic, very little information is available on which Chinese company actually makes these products. much is known: This Wavlink is a technology company based in Shenzhen, China, in the Guangdong Province. The company has around 1,000 employees and sells its products worldwide. Less information is publicly available about the company Jetstream. It is believed that the manufacturer behind the name is Winstars.

I suspect that currently only a few of these devices can be found in German-speaking countries (but I may be mistaken). For more details, see this article by Lee, the video above, and the article on CyberNews .

Similar articles:

Will the router compulsion come back?
Tip: Router Security Test Pages
Fraunhofer test: security deficiencies in home routers
More Telekom business routers with security bug (11/27/2019)
Router vulnerabilities (D-Link, Cable Haunt, India)
Attacks on DrayTrec routers endanger company networks
List of D-Link routers with unfixed RCE vulnerabilities
Cisco security update for switches and routers

This entry was under Devices , Security filed and Router , Security tagged . Bookmark the permalink .

19 responses to *backdoor in Chinese routers (Jetstream, Wavelink, Ematic)*

Michael Bickel *says:*
November 24, 2020 at 11:33 am

... are you surprised? I'm always amazed at how naively many users choose certain products as long as the price and technology are right, especially blatant in the area of smartphones. Probably not infrequently the same users who install questionable ad blockers and are terribly upset about data collection by Microsoft or others.

answers

> **ralf** *says:*
> November 24, 2020 at 12:29 pm
>
> However, the price and reputation of the manufacturer are no guarantees for secure systems:
>
> https://de.wikipedia.org/wiki/Cisco_Systems#Spionage-Vorw%C3%BCrfe
> https://de.wikipedia.org/wiki/Juniper_Networks#Juniper-Skandal
> https://de.wikipedia.org/wiki/Netgear#Spionage-Vorw%C3%BCrfe
> https://de.wikipedia.org/wiki/D-Link#Sicherheitsproblematik
> https://de.wikipedia.org/wiki/Belkin_International#Backdoor-Problematik_bei_Linksys-Routern
> …
>
> answers
>
> > **mw** *says:*
> > November 25, 2020 at 7:56 am
> >
> > Yes, I think it's crazy too. With the iPhone, the price is insanely high for a technology that works but unfortunately goes in the wrong direction. Still, people buy the stuff.
> >
> > Brand or price is not an indicator of quality. Sorry but 'you get shitty here as well as next door'.
> >
> > answers

Günter Born *says:*
November 24, 2020 at 11:52 am

Is the crux for me as a blogger:

- Those who need it (for example because they buy it from MM's grabber box) do not read the articles here.
- Those who read it here don't need the info ...

Basically it applies to every topic - today it became clear to me again regarding the comments on the WIM size problem.

Under that aspect, I could largely stop reporting. But apparently I'm doing it right as a blogger if I post separating topics here anyway ;-).

Let's see, maybe I'll get into the car right away and 'drive into the sun' - a few kilometers further, the lies Feldberg im Taunus (881 meters high) above the layer of fog and has clear, blue skies with 16 km foresight ...

answers

> **Dat Bundesferkel** *says:*
> November 24, 2020 at 1:40 pm
>
> I'll speak for myself now: Even if I don't comment on an article, I read it (and usually find it interesting). If I have nothing to say, however, I think like Dieter Nuhr. Ergo: quiet connoisseur. : D
>
> And as you suspected: Yes, I would not voluntarily bring such a router into my home, but ... you will meet friends again who access something like that. You can then refer to your blog (among other things). ;)
>
> At home I only use *** with routers. But that's because, due to the technology, I don't have the largest selection options - and bridging doesn't come in my bag, see my colleague how smoothly it works ...
>
> answers
>
> > **Thomas** *says:*
> > November 24, 2020 at 7:50 pm
> >
> > "Scribble" box…?
> > Günter, control your fingers. :-)

It should be called "Grabbelkiste".

answers

> **Günter Born** *says:*
> November 25, 2020 at 9:01 am
>
> Corrected it - thanks, Siggi Freud hit through with the grandchildren's crawling box ;-).
>
> answers

1ST1 says *:*
November 25, 2020 at 12:11 am

With a little lead time, the Feldberg could be implemented, then we could run into each other up there on neutral ground, so to speak.

answers

Bachmann *sagt:*
November 25, 2020 at 11:53 am

There are also people "in between". Who do not use the MM grab boxes, but are also not IT professionals. They just want to keep their work equipment, e.g. a PC, safe and functional.
And they can find very useful information here.

answers

Blupp *says:*
November 24, 2020 at 12:25 pm

The idea with the "Reinheitsgebot" is certainly intended in the right direction.
Projects like OpenWrt and DD-Wrt are certainly a viable option here and maybe the last resort for these devices, if they are supported.

answers

No *says:*
November 24, 2020 at 1:06 pm

Is there a list of router MAC addresses? (Usually identifies the manufacturer)

How can you recognize the backdoor? Which ports are used for communication?

What about access points that do not assign their own IP address?

answers

> **Dat Bundesferkel** *says:*
> November 24, 2020 at 1:50 pm
>
> "Is there a list of router MAC addresses? (Usually identifies the manufacturer)"
> About the pencil:
>
> https://www.adminsub.net/mac-address-finder/jetstream
>
> answers

No *says:*
November 24, 2020 at 1:43 pm

It can be even more stupid:

https://www.welivesecurity.com/2020/11/23/security-flaws-smart-doorbells-open-door-hackers/

The question remains, why does someone buy such devices.

answers

> **Dat Bundesferkel** *says:*

November 24, 2020 at 1:49 pm

"The question remains, why does someone buy such devices."
Because everyone else is holding up progress and is forever yesterday. Don't you know the typical reactions of IoT fans? They are also not interested in the fact that ABUS still delivered some of its security products (OEM) with fixed root: toor access data. It's not that wild, all critics wear aluminum hats.

answers

Hartmut *says:*
November 24, 2020 at 4:56 pm

How does it work with routers from Telekom, for example the Speedport w 724 V? The manufacturer is the Chinese company Huawei, as I have found out. Possibly there are also backdoors there? I don't wear an aluminum hat, but you can ask. Maybe someone has an answer for that.
Greetings Hartmut

answers

Günter Born *says:*
November 24, 2020 at 5:11 pm

There was something there in 2014 ...

SP W 724V Type C also with backdoor?
Mysterious backdoor in various router models
Stay away from the Telecom router Speedport W 724V

But they are certainly no longer today's devices that are made available as 'Speedport w 724 V'. Here in the blog, the router was only noticed because it blocked the online loan.

answers

Dat Bundesferkel *says:*
November 24, 2020 at 5:24 pm

Which manufacturer it is depends on the EXACT model (aka type):

Typ A: Huawei
Typ B: Arcadyan
Typ C: Sercomm

At the time, it was suspected that the type C had a backdoor. I can't answer that directly as to whether one is really true.

You can try your luck with the network check from heise:
https://www.four.heise.de/security/dienste/portscan/test/do.shtml?scanart=1&ports=&rm=scan&submit=Scan+starten

answers

---

mw *says:*
November 25, 2020 at 7:50 am

"I only let AVM routers in my four walls". To answer with the Monaco Franze: definitely not!
Because AVM routers offer no guarantee. And the TR-069 management of the provider allows soagr without back doors that the router can be penetrated and thus of course also into the network behind it.

Routers are only allowed to have open source software with me. A frit is only good as a modem or network termination.

answers

Dat Bundesferkel *says:*
November 25, 2020 at 5:17 pm

You can deactivate TR-069 in the purchase routers. Only the loan boxes hide this option from the customer. Also one of the reasons to replace rental boxes.

But yes, AVM is not the ultimate answer. The software is partly ancient and insecure, but you don't have too much of a choice if you have a cable connection. Bridging, on the other hand, is often associated with a loss of performance (VF), which makes it difficult to "connect in series" between the provider modem and a "good" router.

answers

Hinweis: Bitte *beachtet die Regeln* zum Kommentieren im Blog (Erstkommentare und Verlinktes landet in der Moderation, gebe ich alle paar Stunden frei, SEO-Posts/SPAM lösche ich rigoros). Kommentare abseits des Themas bitte unter Diskussion.
