10 Jul 2020 -12:10

CCB issues warning about potential Ransomware attack

The Centre for Cybersecurity Belgium (CCB) received information from a reliable source which indicates that an unidentified vulnerability is being exploited in DrayTek routers enabling ransomware attackers to access thousands of corporate networks worldwide.

A study by the Centre for Cyber Security Belgium (CCB) shows that DrayTek Vigor2960 routers are affected by the unidentified vulnerability, whilst other DrayTek devices are likely impacted.

The vulnerability allows attackers to bypass the authentication procedures and remotely inject or execute code on the operating system of the DrayTek Vigor2960 routers.

DrayTek has developed patches for some recently disclosed security vulnerabilities, however, it is not clear whether the aforementioned exploited vulnerability has been patched. Nevertheless, the CCB strongly recommends that users perform the latest security updates on DrayTek routers.

Checking for backdoors

The CCB has performed penetration tests, showing that previously installed backdoors on DrayTek Vigor2960 routers using version 1.4 of the firmware were not removed after patching to version 1.5.1.1. This suggests that a compromised router will remain compromised even after upgrading to version 1.5.1.1.

> " "We call on companies to update affected devices and check for backdoors. The implementation of DrayTek's security update in this case does not guarantee that you will no longer be vulnerable to a potential ransomware attack. If hackers were able to install backdoors prior to the update, you will still be vulnerable after the patch". "
>
> Pedro Deryckere
> Centre for Cybersecurity Belgium

CCB contacted its constituents with a specific security alert with the description, possible consequences and possible solutions of the vulnerability and threat.

Courses of Action:

- Always back up your configuration before doing an upgrade.
- Upgrade your devices immediately 'and monitor for any newly available patches for the DrayTek devices.
- After upgrading, do check that the web interface now shows the new firmware version.
- Check that no additional remote access profiles (VPN dial-in, teleworker or LAN to LAN) or admin users (for router admin) have been added.
- Check if any ACLs (Access Control Lists) have been altered.
- Disable the remote access on your router if you don’t need it.
- Disable remote access (admin) and SSL VPN. The ACL does not apply to SSL VPN connections (Port 443) so you should also temporarily disable SSL VPN until you have updated the firmware.
- Enable syslog logging for monitoring if there are abnormal events.

The CCB contacted and informed DrayTek. DrayTek did not respond.

Ransomware is on the rise.

Ransomware is a virus that is installed on a device without the owner's consent and demands a ransom in exchange for unlocking the device and files.

Anyone can fall victim to ransomware: private individuals, independent professionals, hospitals and even large companies and the government.

You can protect yourself against ransomware.

For every internet user:

- It is important to protect your devices with antivirus software, but also specific protection against ransomware has become a must.
- Also, it is still very important to identify fake messages in time and to perform regular updates on all your systems.
- Finally, make regular backups in case you are attacked.

For companies and organisations:

- The recommendations for every internet user are of course also important for companies and organisations, but we advise them to go a step further.
- For SMEs and the self-employed, Endpoint protection software may be sufficient. But for large companies, a specialized business anti-ransomware solution is recommended.
- Provide a business continuity and recovery plan with a tested backup system.

- Make sure your organisation is prepared for a cyber-attack. Check out our webinar.
- Have your IT security architecture & policy reviewed by a specialist (including policies on patching, user training, network segmentation, etc.).
- Work on a cybersecurity strategy. Read how to do this here.

Private individuals can find all the tips they need to protect themselves against ransomware at www.safeonweb.be.

Organisations and companies can visit www.CERT.be. We published the white paper 'ransomware: protection and prevention' in September 2019. This whitepaper was updated in 2020.

Centre for Cyber Security Belgium
Rue de la Loi 16
1000 Brussels
Belgium
http://www.ccb.belgium.be

Andries Bomans
Communications officer
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - momenteel in verlof Eggers - momenteel in verlof
Communications officer
+32 485 76 53 36
katrien.eggers@cert.be