Unauthenticated RCE in Draytek Vigor 2960, 3900 and 300

CVE-2020-8515

Severity: 9.8 critical
Discovered by: Matías Peters
Date: Mar 30 2020

Description

Vulnerabilty Type: Remote Code Execution

Affected:

- DrayTek Vigor2960 1.3.1_Beta
- Vigor3900 1.4.4_Beta
- Vigor300B 1.3.3_Beta
- Vigor300B 1.4.2.1_Beta
- Vigor300B 1.4.4_Beta

Founded in 1997, DrayTek Corporation (Chinese: 居易科技) is a Taiwan-based manufacturer of networking equipment and management systems - from ISDN, VDSL to LTE[1]. A critical vulnerability affecting DrayTek Vigor enterprise switches, load-balancers, routers and VPN gateway devices has been discovered, allowing for remote code execution as root (without authentication) via shell metacharacters to the cgi-bin/mainfunction.cgi URI.
This issue has been fixed in Vigor3900/2960/300B v1.5.1.

Attack Vector

In the course of investigating various telecommunication brands, Draytek's vulnerability was detected. The vulnerability allows intruders to take full control of the device remotely without the need for authentication on the site.

To verify the exposure, we ran a "ID" test that allowed us to identify which user was running the application.

Impact

Our research team discovered that by default, Draytek was running this service with the "root" user which has high privileges in the operating system, making the vulnerability critical (9.8 severity).

[1] https://www.draytek.com/about/about-draytek/

Mitigations

On February 2020, DrayTek published the vulnerability and the update needed to patch it: https://www.draytek.com/about/security-advisory/vigor3900-/-vigor2960-/-vigor300b-router-web-management-page-vulnerability-(cve-2020-8515)/

Model	Fixed Version	Download Link
Vigor300B	1.5.1	https://www.draytek.com.tw/ftp/Vigor300B/Firmware/v1.5.1/
Vigor2960	1.5.1	https://www.draytek.com.tw/ftp/Vigor2960/Firmware/v1.5.1/
Vigor3900	1.5.1	https://www.draytek.com.tw/ftp/Vigor3900/Firmware/v1.5.1/

Recommendation

Affected companies and individuals are highly advised to install the latest firmware updates to completely protect their valuable networks against malware and emerging online threats. We recommend that DrayTek Vigor users check and update their firmware to 1.5.1 as soon as possible.

References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8515
https://nvd.nist.gov/vuln/detail/CVE-2020-8515#vulnCurrentDescriptionTitle
https://www.skullarmy.net/2020/01/draytek-unauthenticated-rce-in-draytek.html

DREAMLAB TECHNOLOGIES AG

Dreamlab is a pioneer in information security. We have been analysing and securing cyberspace for 20 years. As an independent, neutral, globally active Swiss organisation, we define future standards for cyber defence and IT security milestones. Research, analysis and forensics are giving rise to innovative security solutions for customers with increased security requirements.

Dreamlab Technologies AG is a leader in the development and implementation of individual solutions for the integral security of information, organisations and systems. As a performance-oriented partner, Dreamlab offers advice, au- dits, solutions and know-how transfer, while being commit- ted to objectively verifiable security, based on open stan- dards.

dreamlab.net

MATIAS PETER, Security Consultant

Network Engineer and Master in Cybersecurity with experience in second factor authentication platforms and firewall's policy optimization in transactional customers and currently working as a Security Consultant @ Dreamlab Technologies, focused in pentesting proyects.