



NCSC-2024-0388

Kwetsbaarheden verholpen in Draytek Vigor routers

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 04-10-2024

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Draytek heeft kwetsbaarheden verholpen in diverse typen routers uit de Vigor-serie.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, of om een Cross-Site-Scripting-aanval uit te voeren en daarmee mogelijk toegang te krijgen tot gevoelige gegevens of willekeurige code uit te voeren in de context van de browser van het slachtoffer.

Voor een succesvolle Cross-Site-Scripting, en daarmee uitvoer van code, moet de kwaadwillende toegang hebben tot de web-interface van het kwetsbare systeem. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheer-omgeving.

Kwetsbare systemen van de types

- Vigor2620
- VigorLTE200
- Vigor2133
- Vigor2762
- Vigor2832
- Vigor2860
- Vigor2925
- Vigor2862
- Vigor2926
- Vigor2952
- Vigor3220

zijn End-of-Life en ontvangen geen beveiligingsupdates. Draytek levert nog wel één patch voor de kwetsbaarheid met kenmerk CVE-2024-41592. De overige kwetsbaarheden worden niet (meer) verholpen.

Oplossingen

Draytek heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Tevens wijst het NCSC erop dat een deel van de kwetsbare systemen End-of-Life is en uitsluitend een fix heeft gekregen voor de kwetsbaarheid met kenmerk CVE-2024-41592. Het NCSC adviseert deze systemen te vervangen voor modernere en ondersteunde systemen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://www.forescout.com/resources/draybreak-draytek-research/>
- <https://www.draytek.com/support/resources/routers#version>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-41583	
➤ CVE-2024-41584	
➤ CVE-2024-41585	
➤ CVE-2024-41586	
➤ CVE-2024-41587	
➤ CVE-2024-41588	
➤ CVE-2024-41589	
➤ CVE-2024-41590	
➤ CVE-2024-41591	
➤ CVE-2024-41592	
➤ CVE-2024-41593	
➤ CVE-2024-41594	
➤ CVE-2024-41595	
➤ CVE-2024-41596	

CWE's

CWE	Beschrijving
➤ CVE-319	Cleartext Transmission of Sensitive Information

➤ CWE-121	Stack-based Buffer Overflow
➤ CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

draytek
vigor310
vigor3910

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.