Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0327

Kwetsbaarheden verholpen in DrayTek VigorAP

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 26-08-2026

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 meerdere kwetsbaarheden verholpen in de VigorAP productlijn.

Duiding

De kwetsbaarheden bevinden zich in verschillende functies en componenten van de DrayTek VigorAP apparaten, waaronder tr069TestInform, ExportSettings, setLan, setcamset, mesh_start_speed_test, InquierTime, apautotest, upload_settings.cgi en dray_apm. Deze kwetsbaarheden maken het mogelijk voor aanvallers met geldige authenticatie om via onvoldoende inputvalidatie en filtering willekeurige commando's uit te voeren met root-privileges. Daarnaast is er sprake van buffer overflow kwetsbaarheden in de setLan en apautotest functies, waarbij door het versturen van speciaal vervaardigde input een denial of service kan worden veroorzaakt of willekeurige code kan worden uitgevoerd. Exploitatie van deze kwetsbaarheden kan leiden tot volledige systeemcompromittering binnen de context van de root gebruiker. De kwetsbaarheden zijn specifiek van toepassing op meerdere modellen binnen de DrayTek VigorAP productlijn.

Oplossingen

DrayTek heeft updates uitgebracht om de kwetsbaarheden in de VigorAP apparaten te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.draytek.com/about/security-advisory/multiple-remote-code-execution-and-buffer-overflow-vulnerabilities-in-vigorap-series-august-2026
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-buffer-overflow-via-apautotest
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-buffer-overflow-via-setlan
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-apautotest
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-exportsettings
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-inquiertime
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-mesh-start-speed-test
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-setcamset
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-setlan
- https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-tr069testinform

› https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-os-command-injection-via-upload-settings-cgi
› https://www.vulncheck.com/advisories/draytek-vigorap-multiple-models-pre-authentication-os-command-injection-via-dray-apm

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-71904	8.6 HIGH
› CVE-2026-71905	8.6 HIGH
› CVE-2026-71906	8.6 HIGH
› CVE-2026-71907	8.6 HIGH
› CVE-2026-71908	8.6 HIGH
› CVE-2026-71909	8.6 HIGH
› CVE-2026-71910	8.6 HIGH
› CVE-2026-71911	8.6 HIGH
› CVE-2026-71912	8.6 HIGH
› CVE-2026-71913	8.6 HIGH
› CVE-2026-71914	9.3 CRITICAL

CWE's

CWE	Beschrijving
› CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
› CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Getroffen producten

DrayTek
Vigor
Draytek
VigorAP 1060c Firmware
VigorAP 700 Firmware
VigorAP 800 Firmware
VigorAP 802 Firmware
VigorAP 900 Firmware
VigorAP 902 Firmware
VigorAP 910C Firmware
VigorAP 912C Firmware
VigorAP 918R Firmware
VigorAP 920R Firmware
Vigorap 1000C Firmware
Vigorap 903 Firmware
Vigorap 960C Firmware

Disclaimer