Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0328

Kwetsbaarheden verholpen in DrayTek VigorSwitch

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 VigorSwitch productlijn.

Duiding

De kwetsbaarheden betreffen voornamelijk command injection, buffer overflow, null pointer dereference, directory traversal en onvoldoende autorisatiecontroles in diverse functies van de DrayTek VigorSwitch apparaten. Command injection kwetsbaarheden bevinden zich onder andere in functies zoals jsonstatus, commandTable, pingtrace, webBackupAction, sysreboot, auth_set, getVid, getDetail, setDevice, rebDevice, fdftDevice, setDevProto, setTime, tftp_upgrade en setDevNet. Deze maken het mogelijk voor een aanvaller om willekeurige commando's met root privileges uit te voeren. Sommige command injection kwetsbaarheden zijn pre-authenticatie, zoals in de setget.cgi interface, waardoor geen voorafgaande authenticatie vereist is voor exploitatie.

Buffer overflow kwetsbaarheden zijn aanwezig in functies zoals pingtrace, webBackupAction, sysreboot, poe_schedule_profile, switch_lan_gvrp, acl_general_setup Add ACE en Edit ACE, diag_logmail en mail_mailalert. Deze kunnen leiden tot denial of service of uitvoering van willekeurige code onder administratieve rechten.

Null pointer dereference kwetsbaarheden in formlogout en setget.cgi kunnen leiden tot een denial of service door het crashen van de service.

Directory traversal in getSyslogFile maakt het mogelijk om, mits geauthenticeerd, toegang te krijgen tot willekeurige bestanden op het systeem. Onvoldoende autorisatiecontroles in syslog functies stellen een aanvaller in staat om configuraties te wijzigen, services te herstarten, configuraties op te slaan of logs te wissen zonder de juiste rechten.

Exploitatie van deze kwetsbaarheden vereist in de meeste gevallen geldige administratieve credentials, behalve bij de pre-authenticatie command injection en null pointer dereference in setget.cgi.

Oplossingen

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

Referenties

- https://www.draytek.com/about/security-advisory/multiple-vulnerabilities-in-vigorswitch-series-august-2026
- https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-acl-general-setup-add-ace

› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-acl-general-setup-edit-ace
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-diag-logmail
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-mail-mailalert
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-pingtrace
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-poe-schedule-profile
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-switch-lan-gvrp
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-sysreboot
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-buffer-overflow-via-webbackupaction
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-missing-authorization-in-syslog-functions
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-null-pointer-dereference-via-formlogout
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-auth-set
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-commandtable
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-fdftdevice
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-getdetail
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-getvid
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-jsonstatus
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-pingtrace
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-rebdevice
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-setdevice
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-setdevnet
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-setdevproto
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-

settime
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-sysreboot
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-tftp-upgrade
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-os-command-injection-via-webbackupaction
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-path-traversal-via-getsyslogfile

› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-pre-authentication-null-pointer-dereference-via-setget-cgi
› https://www.vulncheck.com/advisories/draytek-vigorswitch-multiple-models-pre-authentication-os-command-injection-via-setget-cgi

Kwetsbaarheden

CVE	CVSS Score
› CVE-2026-71915	8.6 HIGH
› CVE-2026-71916	8.6 HIGH
› CVE-2026-71917	8.6 HIGH
› CVE-2026-71918	8.6 HIGH
› CVE-2026-71919	8.6 HIGH
› CVE-2026-71920	6.9 MEDIUM
› CVE-2026-71921	9.3 CRITICAL
› CVE-2026-71922	8.7 HIGH
› CVE-2026-71923	8.6 HIGH
› CVE-2026-71924	8.6 HIGH
› CVE-2026-71925	8.6 HIGH
› CVE-2026-71926	8.6 HIGH
› CVE-2026-71927	8.6 HIGH

CVE-2026-71928	8.6 HIGH
CVE-2026-71929	8.6 HIGH
CVE-2026-71930	8.6 HIGH
CVE-2026-71931	8.6 HIGH
CVE-2026-71932	6.9 MEDIUM
CVE-2026-71933	8.8 HIGH
CVE-2026-71934	8.6 HIGH
CVE-2026-71935	8.6 HIGH
CVE-2026-71936	8.6 HIGH
CVE-2026-71937	8.6 HIGH
CVE-2026-71938	8.6 HIGH
CVE-2026-71939	8.6 HIGH
CVE-2026-71940	8.6 HIGH
CVE-2026-71941	8.6 HIGH
CVE-2026-71942	8.6 HIGH
CVE-2026-71943	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
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')
CWE-476	NULL Pointer Dereference

CWE-862	Missing Authorization

Getroffen producten

DrayTek
Vigor
DrayTek Corporation
VigorSwitch FX2120
VigorSwitch G1280
VigorSwitch G1282
VigorSwitch G2100
VigorSwitch G2121
VigorSwitch G2280x
VigorSwitch G2282x
VigorSwitch G2540x
VigorSwitch G2540xs
VigorSwitch G2542x
VigorSwitch P1280
VigorSwitch P1281x

VigorSwitch P1282
VigorSwitch P2100
VigorSwitch P2121
VigorSwitch P2280x
VigorSwitch P2282x
VigorSwitch P2540x
VigorSwitch P2540xs
VigorSwitch P2542x
VigorSwitch P2542xh
VigorSwitch PQ2121x
VigorSwitch PQ2200xb
VigorSwitch PQ2300xb
VigorSwitch PX2060
VigorSwitch Q2121x
VigorSwitch Q2200x
VigorSwitch Q2300x

Disclaimer