

CVE-2020-15415

DrayTek Multiple Vigor Routers OS Command Injection Vulnerability

CISA KEV since Sep 30, 2024

Actively exploited

On DrayTek Vigor3900, Vigor2960, and Vigor300B devices before 1.5.1, cgi-bin/mainfunction.cgi/cvmcfcgupload allows remote command execution via shell metacharacters in a filename when the text/x-python-script content type is used, a different issue than CVE-2020-14472.

EVRS 83 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.845 99.7th percentile · FIRST	CISA DEADLINE Oct 21, 2024 KEV since 2024 · listed over a year
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.845 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
vigor3900 firmware	< 1.5.1	1.5.1	NVD
vigor2960 firmware	< 1.5.1	1.5.1	NVD
vigor300b firmware	< 1.5.1	1.5.1	NVD
vigor3900	–	no fixed version listed	NVD
vigor2960	–	no fixed version listed	NVD
vigor300b	–	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-65hg-r7rx-55rg
draytek.com [draytek.com/about/security-advisory/vigor3900/-vigor2960/-vigor300b-remote-code-injection/execution-vulnerability-\(cve-2020-14472\)](https://draytek.com/about/security-advisory/vigor3900/-vigor2960/-vigor300b-remote-code-injection/execution-vulnerability-(cve-2020-14472))
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2020-15415

Additional guidance draytek.com/about/security-advisory
NVD nvd.nist.gov/vuln/detail/CVE-2020-15415
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-7408

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.