Alessandro Sgreccia

Independent security researcher, online as **rainpwn**.
Network security appliances, from the web interface down to the firmware.

rainpwn.blog
rainpwn@protonmail.com
github.com/rainpwn
linkedin.com/in/rainpwn
infosec.exchange/@rainpwn
PGP on rainpwn.blog/contact

20	3	9.8	13	7
CVES ASSIGNED	VENDORS	HIGHEST CVSS	WRITEUPS	PUBLIC POCS

PROFILE

I test network security appliances: firewalls, access points, security routers, and the firmware they run. I start at the web management interface, because that is what is exposed, then follow the same request into the CLI, the services it runs as root, and the firmware image. Most of what I find sits between two of those layers. Everything goes to the vendor first, and I publish once the fix ships.

EXPERIENCE

Hackerhood, Red Hot Cyber Security researcher — July 2023 – present

Independent research Vulnerability research, reverse engineering, exploit development — 2022 – present

ASSIGNED CVES

IDENTIFIER	CLASS	PRODUCT	CVSS	SEVERITY
CVE-2022-0342	Authentication bypass	USG/ZyWALL, USG FLEX, ATP, VPN, NSG	9.8	Critical
CVE-2023-27991	Command injection	ATP, USG FLEX, USG20(W)-VPN, VPN	8.8	High
CVE-2024-12398	Privilege escalation	22 NWA/WAC/WAX/WBE APs, USG LITE 60AX	8.8	High
TBA	Remote code execution	UaniaBOX, UaniaOS ≥2.1 <3.0.1	8.8	High
CVE-2025-9133	Authentication bypass	ATP, USG FLEX, USG20(W)-VPN	8.2	High
CVE-2024-9677	Privilege escalation	USG FLEX H	7.8	High
CVE-2025-1731	Remote code execution	USG FLEX H	7.8	High
CVE-2024-7203	Command injection	ATP, USG FLEX	7.2	High
CVE-2025-8078	Command injection	ATP, USG FLEX, USG20(W)-VPN	7.2	High
CVE-2025-11730	Command injection	ATP, USG FLEX, USG20(W)-VPN	7.2	High
CVE-2025-1732	Privilege escalation	USG FLEX H	6.7	Medium

IDENTIFIER	CLASS	PRODUCT	CVSS	SEVERITY
CVE-2024-1575	Privilege escalation	20 NWA/WAC/WAX/WBE access points	6.5	Medium
CVE-2022-40603	Cross-site scripting	ATP, USG FLEX, VPN, ZyWALL/USG	6.1	Medium
CVE-2023-37925	Information disclosure	ATP, USG FLEX, USG20(W)-VPN, VPN + 20 APs	5.5	Medium
CVE-2023-37926	Buffer overflow	ATP, USG FLEX, USG20(W)-VPN, VPN	5.5	Medium
CVE-2023-5650	Open redirect	ATP, USG FLEX, USG20(W)-VPN, VPN	5.5	Medium
CVE-2023-5797	Information disclosure	ATP, USG FLEX, USG20(W)-VPN, VPN + 20 APs	5.5	Medium
CVE-2023-5960	Information disclosure	USG FLEX, VPN	5.5	Medium
CVE-2023-27990	Cross-site scripting	ATP, USG FLEX, USG20(W)-VPN, VPN	4.8	Medium
CVE-2023-4397	Buffer overflow	ATP, USG FLEX, USG20(W)-VPN	4.4	Medium

All **20 findings**, on network appliances from three vendors between 2022 and 2026: one critical, nine high, ten medium, every one patched. Nineteen carry a CVE; the UANIA identifier is still pending at MITRE, with the advisory already public. One further advisory is published and fixed with no identifier, **Breldo Italia** (GHUMI-2026-01). Writeups and proof of concepts on rainpwn.blog.

DISCLOSURE RECORD

COVERAGE	**20 of 20** carry a vendor advisory and are patched. Nineteen are on NVD.
TIMING	Median **67 days** from report to public advisory, across eleven dated timelines published on the site.
THE VENDOR DECIDES	Four times a vendor asked to postpone a disclosure. **Four times I waited.** The longest hold was 148 days.
RETEST	One patch did not hold. I applied it, found the issue still worked, and **reported it again**.

FOCUS

LAYERS	Web management interface, CLI and shell, services running as root, firmware images.
CLASSES FOUND	Command injection (4), privilege escalation (4), information disclosure (3), authentication bypass (2), buffer overflow (2), cross-site scripting (2), remote code execution (2), open redirect (1).
RECOGNITION	**ZYXEL Hall of Fame**.
LANGUAGES	English, Italian.