PUBLIC PREVIEW, FULL BRIEF AVAILABLE TO CUSTOMERS

AT THE EDGE

Weekly Intelligence Brief

A Dormant Palo Alto GlobalProtect RCE Returned to Active Exploitation

GreyNoise recorded a sharp resurgence in exploitation attempts against Palo Alto GlobalProtect CVE-2019-1579 (CISA KEV, unauthenticated RCE): only isolated activity through late June, then more than 120 malicious hosts on the evening of 06 July, almost all from a single hosting network. Separately, two coordinated hosting fleets ran the week's highest-volume web exploitation.

GlobalProtect
PALO ALTO KEV RCE (CVE-2019-1579) WENT FROM DORMANT TO 120+ MALICIOUS HOSTS ON 06 JULY

CISA KEV
THE RESURGENT GLOBALPROTECT FLAW IS AN UNAUTHENTICATED RCE WITH PUBLIC EXPLOIT CODE

100+ Hosts
TWO COORDINATED HOSTING FLEETS RAN THE WEEK'S HIGHEST-VOLUME WEB EXPLOITATION

Credentials
THE FLEETS' OBJECTIVE: HARVESTING EXPOSED .ENV, GIT, AND CLOUD-CONFIG FILES

WHAT'S INSIDE

1 A Palo Alto GlobalProtect KEV flaw returned to active exploitation

CVE-2019-1579 (unauthenticated RCE, CISA KEV) drew more than 120 malicious hosts on 06 July after only isolated activity in late June, almost all from a single hosting network. Any internet-facing GlobalProtect portal on vulnerable firmware is in scope.

2 Two coordinated hosting fleets ran the highest-volume activity

TECHOFF (AS48090, Netherlands) and Bucklog SARL (AS211590, France) together ran roughly 7.5 million connection attempts on a shared web-exploitation and credential-harvesting toolkit, with 129 hosts classified malicious and 30 suspicious. The CVEs are commodity; the coordination runs at provider scale.

3 Credential harvesting was the fleets' objective

ENV Crawler, the automated hunt for exposed .env files, logged 4.76 million requests across the sensor network, with Git, cloud-config, and PHP-info file requests close behind. A config file that returns content yields working credentials with no exploitation required.

4 Detection is behavioral

Across all of this week's activity, the source addresses rotate but the exploitation patterns and client fingerprints do not. Patch the GlobalProtect flaw, block the fleets at the network-block level, and detect on behavior rather than a static IP list.

Want the full brief?

GreyNoise customers get complete IOCs, infrastructure attribution, and role-based recommendations every week.

greynoise.io/contact