UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00224

PALO ALTO VPN/FIREWALL CRITICAL VULNERABILITY

DATE ISSUED: 17th November 2021

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	**MEDIUM**	EASY

OVERVIEW

Critical Zero-Day vulnerability discovered in Palo Alto's GlobalProtect enabled Firewalls, which also handles VPN access, potentially allowing unauthenticated users to remotely execute code, affecting thousands of devices s being tracked as CVE 2021-3064 (rated 9.8/10 CVSS) and has recently been patched by the vendor.

BREAKDOWN

Affecting both the physical and virtual appliances running versions prior to 8.1.17, and advisory and a patch have been issued by Palo Alto (see resources below) to combat the zero-day vulnerability affecting its PAN-OS operating system for security devices. If successfully exploited, an unauthenticated attacker could access sensitive configuration and credential data on targeted devices and use this to gain visibility and move across a network. Randori researchers believe that there are possibly "more than 70,000 vulnerable instances exposed on internet-facing assets." Accessed through the default 443 port, a buffer overflow and HTTP smuggling attacker when used in conjunction can gain a malicious actor privilege enabling them to perform Remote Code Execution (RCE) on the targeted system. Exploit code is not publicly available at this stage.

REMEDIATION STEPS

- Update Palo Alto virtual and hardware firewalls to the latest version to apply the new security patches
- Apply threat signatures 97820 and 91855 released by Palo Alto
- If you are not using the VPN component of the firewall, disable GlobalProtect.

REFERENCES & RESOURCES

Palo Alto	https://security.paloaltonetworks.com/CVE-2021-3060
Threatpost	https://threatpost.com/massive-zero-day-hole-found-in-palo-alto-security-appliances/176170/
CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/critical-vulnerability-in-palo-alto-vpn/