How Corvus Alerts Work

Palo Alto Networks VPN Vulnerability

Our Risk + Response team has developed a holistic approach including continual risk assessment, proactive risk management, and rapid response that helps policyholders prevent, prepare for and recover from cyber incidents. A key fixture of our outreach is vulnerability alerts, sent in response to critical security advisories.

Who do we alert, why does it matter, and how do we stay ahead of threat actors? Follow the timeline of one event from the discovery of a vulnerability to the alert landing in a policyholder's inbox:

12:30pm

The Vulnerability is Discovered

On November 10th, 2021, Palo Alto Networks (PAN) issued a security advisory regarding a critical vulnerability, CVE-2021-3064, that affects their firewalls using the GlobalProtect Portal VPN.

> **Potential Impact**
> Threat actors could leverage this vulnerability to gain access to the firewall and VPN device, which is a common target to ultimately deploy ransomware throughout the environment. This was a "zero-day": once the word got out, threat actors were armed with the knowledge of how to seek out vulnerable organizations and launch an attack.

2:30pm

Triage

Our team swiftly responded to the news by engaging our in-house security experts to assess the risk. With numerous advisories announced on any given day, prioritization is critical. Using our established criteria, the team determined that the PAN vulnerability's severity justified a proactive alert to policyholders. Members of the Risk + Response team gathered all known information and compiled it into easy-to-follow instructions that were published by 2:30pm.

6:00pm

The Race to the Inbox (with the help of technology)

With a "zero-day" vulnerability, timely alerts are particularly crucial. But sending alerts that aren't applicable to a policyholder is a waste of their time and risks making them less responsive to true threats. So a key part of determining our response is finding out how many policyholders use the device, and who they are.

> **How do we know who to alert?**
> With the proprietary Corvus Scan, the Corvus Data Science team plugs gaps in traditional "off the shelf" IT scans. One feature utilizes keywords to match certain VPNs, enabling our team to identify which of our policyholders were most likely at risk through the use of the affected software.

7:00pm

Alerts Sent

Within 7 hours of the news breaking, we had alerted any potentially impacted policyholders, and the team stood by to help any policyholders with questions or clarifications. Formal notification from the U.S. CISA took another full day to appear.

> Thank you very much for this information! What a great service. I've just submitted a ticket...
> – SVP of Production, Construction/Contracting Firm

> Thank you very much for the notification, it is wonderful to know we have another layer of security awareness with Corvus
> – IT Manager, Logistics and Wholesale Supply Company

Speed Matters

Whenever a new threat is concerned — especially in the instance of zero-day vulnerabilities— awareness is first in a line of critical and timely next steps. Our alerts to policyholders include the context of what they need to know and the actions they should take to protect their organization, like essential updates and patches.