Zero-Day Disclosure: PAN GlobalProtect CVE-2021-3064

randori.com/blog/cve-2021-3064/

Overview: CVE-2021-3064

On November 10, 2021 Palo Alto Networks (PAN) provided an update that patched CVE-2021-3064 which was discovered and disclosed by Randori. This vulnerability affects PAN firewalls using the GlobalProtect Portal VPN and allows for unauthenticated remote code execution on vulnerable installations of the product. The issue affects multiple versions of PAN-OS 8.1 prior to 8.1.17 and Randori has found numerous vulnerable instances exposed on internet-facing assets, in excess of 10,000 assets.

The Randori Attack Team developed a reliable working exploit and leveraged the capability as part of Randori's continuous and automated red team platform. Our team was able to gain a shell on the affected target, access sensitive configuration data, extract credentials, and

more. Once an attacker has control over the firewall, they will have visibility into the internal network and can proceed to move laterally.

In an effort to avoid enabling misuse, technical details related to CVE-2021-3064 will be withheld from public dissemination for a period of 30 days from the date of this publication. More information will be released at that time. Follow @RandoriAttack on Twitter for updates on future posts.

Key Takeaways

The following are the key takeaways from the Randori Attack Team's discovery and research surrounding this flaw:

- The vulnerability chain consists of a method for bypassing validations made by an external web server (HTTP smuggling) and a stack-based buffer overflow.
- It affects Palo Alto firewalls running the 8.1 series of PAN-OS with GlobalProtect enabled (specifically versions < 8.1.17).
- Exploitation of the vulnerability chain has been proven and allows for remote code execution on both physical and virtual firewall products.
- Publicly available exploit code does not exist at this time.
- Patches are available from the vendor.
  PAN Threat Prevention Signatures are also available (IDs 91820 and 91855) to block exploitation of the issue.
- Public exploit code is likely to surface as:
  - VPN devices are attractive targets for malicious actors, and
  - Exploitation of PA-VM virtual devices in particular is made easier due to their lack of Address Space Layout Randomization (ASLR).

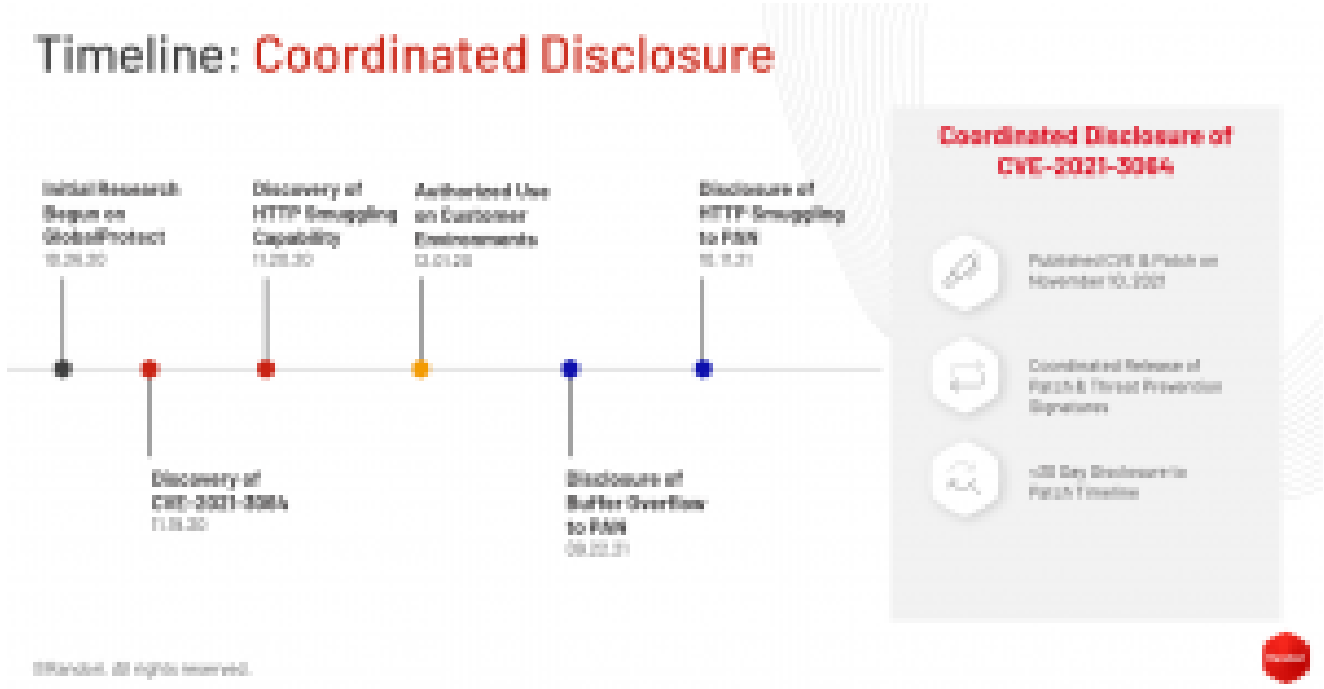
Disclosure Process

This vulnerability was disclosed in accordance with Randori's vulnerability disclosure policy. For more information on Randori's use of non-public capabilities, refer to our blog post Why Zero-Days are Essential to Security.

Timeline

- **2020-10-26:** Randori began initial research on GlobalProtect.
- **2020-11-19:** Randori discovered the buffer overflow vulnerability.
- **2020-11-20:** Randori discovered the HTTP smuggling capability.
- **2020-12-01:** Randori began authorized use of the vulnerability chain as part of Randori's continuous and automated red team platform.
- **2021-09-22:** The buffer overflow vulnerability was disclosed by Randori to PAN.
- **2021-10-11:** The HTTP smuggling capability was disclosed by Randori to PAN.

- **2021-11-10:** PAN released patches and a security bulletin assigning the vulnerability CVE-2021-3064.
- **2021-11-10:** This report was published.



Technical Overview

Detailed technical information usually appearing in our attacker's notes is not provided at this time to allow a period for customers of the affected vendor to patch or upgrade their systems. We will be releasing technical details on December 10, 2021 and hosting a live webinar breaking down the technical details of the exploit on December 14, 2021. Follow @RandoriAttack on Twitter for updates.

Confirmed Exploitable Systems

The Randori Attack team successfully exploited the following systems with GlobalProtect enabled and accessible:

- Palo Alto Networks PA-5220
  - PAN-OS 8.1.16
  - ASLR enabled in firmware for this device
- Palo Alto Networks PA-VM
  - PAN-OS 8.1.15
  - ASLR disabled in firmware for this device

Vulnerability Information

CVE-2021-3064 is a buffer overflow that occurs while parsing user-supplied input into a fixed-length location on the stack. The problematic code is not reachable externally without utilizing an HTTP smuggling technique. Exploitation of these together yields remote code execution under the privileges of the affected component on the firewall device. The smuggling capability was not designated a CVE identifier as it is not considered a security boundary by the affected vendor.

Exploitation

In order to exploit this vulnerability, an attacker must have network access to the device on the GlobalProtect service port (default port 443). As the affected product is a VPN portal, this port is often accessible over the Internet. On devices with ASLR enabled (which appears to be the case in most hardware devices), exploitation is difficult but possible. On virtualized devices (VM-series firewalls), exploitation is significantly easier due to lack of ASLR and Randori expects public exploits will surface. Randori researchers have not exploited the buffer overflow to result in controlled code execution on certain hardware device versions with MIPS-based management plane CPUs due to their big endian architecture, though the overflow is reachable on these devices and can be exploited to limit availability of services.

Mitigation Recommendations

Randori recommends affected organizations apply the patches provided by PAN. Additionally, PAN has made available Threat Prevention signatures 91820 and 91855 that can be enabled to thwart exploitation while organizations plan for the software upgrade. For organizations not using the VPN capability as part of the firewall, we recommend disabling GlobalProtect.

As always, best practices should be followed for any Internet-facing assets, including:

- Monitoring logs and alerts for aberrant activity.
- Restrict originating IP addresses, if possible.
- Applying layered controls such as a web-application firewall, segmentation, and access controls.

References

- **Shodan:** https://www.shodan.io/search/facet?query=http.html%3A%22Global+Protect%22&facet=os
- **Why Zero-Days Are Essential to the Security:** https://www.randori.com/blog/why-zero-days-are-essential-to-security/
- **Palo Alto Networks Security Advisory:** https://security.paloaltonetworks.com/CVE-2021-3064

Update: *This post has been updated to correct the following:*

- *A previous version of this post estimated the number of affected devices at 70,000, this was corrected to 10,000 to reflect updated information.*
- *A typo in the timeline image incorrectly listed the disclosure date of the HTTP smuggling capability as October 2022, this has been corrected to reflect the disclosure date of October 11, 2021.*
- (12/10/21): *On November 10th, we disclosed CVE-2021-3064 in older versions of PAN-OS and announced our intent to release the technical details on December 10th and conduct a webinar on December 14th. We've been collaborating with Palo Alto Networks, who informed us that despite immediate and significant adoption of threat prevention signatures, there are still thousands of customers in the process of applying protections, and are not protected yet. Neither Palo Alto Networks nor Randori's threat intel sources have identified any attempts at exploitation. To help keep Palo Alto Networks' customers secure and Randori's goal of making the overall community safer and more resilient, we have jointly decided to not release technical details at this time.*