TLP: WHITE

Advisory Alert

Alert Number: **AAA20210910** **Date:** **September 10, 2021**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PaloAlto	**High**	Multiple Vulnerabilities
Wordpress	**High**	Multiple Vulnerabilities

Description

Affected Product	PaloAlto
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3051, CVE-2021-3055, CVE-2020-10188, CVE-2021-3052, CVE-2021-3053, CVE-2021-3054, CVE-2021-3049)
Description	Paloalto has released Security Updates addressing multiple vulnerabilities that exists with Paloalto products. **CVE-2021-3051 -** An improper restriction of XML external entity (XXE) reference vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to read any arbitrary file from the file system and send a specifically crafted request to the firewall that causes the service to crash **CVE-2021-3055 -** Vulnerability in the Palo Alto Networks PAN-OS web interface allows an authenticated administrator to read any arbitrary file from the file system. Repeated attempts to send this request result in denial of service to all PAN-OS services by restarting the device and putting it into maintenance mode. **CVE-2020-10188 -** A buffer overflow vulnerability in the Telnet-based administrative management service included with PAN-OS software allows remote attackers to execute arbitrary code. **CVE-2021-3052 -** A vulnerability in the Palo Alto Network's PAN-OS web interface allows an authenticated network-based attacker to trick another into clicking on a link that performs arbitrary actions. **CVE-2021-3053 -** An improper handling of exceptional conditions vulnerability exists in the Palo Alto Networks PAN-OS dataplane that enables an unauthenticated network-based attacker to send specifically crafted traffic through the firewall that causes the service to crash **CVE-2021-3054 -** An authenticated administrator with permission to upload plugins can leverage a time-of-check to time-of-use (TOCTOU) race condition vulnerability in the Palo Alto Networks PAN-OS web interface to execute arbitrary code with root user capabilities. **CVE-2021-3049** - The Palo Alto Networks Cortex XSOAR server improper authorization vulnerability allows an authenticated network attacker with investigation read rights to download data from incident investigations they are aware of but not involved in.
Affected Products	PAN-OS Cortex XSOAR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2021-3051 https://security.paloaltonetworks.com/CVE-2021-3055 https://security.paloaltonetworks.com/CVE-2020-10188 https://security.paloaltonetworks.com/CVE-2021-3052 https://security.paloaltonetworks.com/CVE-2021-3053 https://security.paloaltonetworks.com/CVE-2021-3054 https://security.paloaltonetworks.com/CVE-2021-3049

Affected Product	Wordpress
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	WordPress releases its security and maintenance update in order to address three vulnerabilities including Data exposure vulnerability within the REST API, XSS vulnerability in the block editor.Incorporate upstream security fixes and multiple bug fixes.
Affected Products	WordPress versions between 5.4 and 5.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2021/09/wordpress-5-8-1-security-and-maintenance-release/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.