Advisory Alert

Alert Number: AAA20220210 **Date:** February 10, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	**High**	Multiple vulnerabilities
Zimbra	**High**	Multiple vulnerabilities

Description

Affected Product	Palo Alto
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-0016, CVE-2022-0017, CVE-2022-0020, CVE-2022-0011, CVE-2022-0018, CVE-2022-0019, CVE-2022-0021)
Description	Palo Alto has released updates addressing multiple vulnerabilities that exists in their products such as Privilege Escalation Vulnerability, Local Privilege Escalation, Cross-Site Scripting (XSS), URL Filtering, Information Exposure Vulnerability, Insufficiently Protected Credentials Vulnerability, Information Exposure Vulnerability.
Affected Products	GlobalProtect App 5.2 to 5.2.9 on Windows and MacOS GlobalProtect App 5.2 to 5.2.5 on Windows GlobalProtect App 5.1 to 5.1.10 on Windows Cortex XSOAR 6.2.0 Cortex XSOAR 6.1.0 all PAN-OS 10.1 to 10.1.3 PAN-OS 10.0 to 10.0.8 PAN-OS 9.1 to 9.1.12 PAN-OS 9.0 to 9.0.* PAN-OS 8.1 to 8.1.21 GlobalProtect App 5.2 to 5.2.9 on Windows and MacOS GlobalProtect App 5.1 to 5.1.10 on Windows and MacOS GlobalProtect App 5.3 to 5.3.2 on Linux GlobalProtect App 5.2 to 5.2.7 on Linux GlobalProtect App 5.1 to 5.1.10 on Linux GlobalProtect App 5.2 to 5.2.9 on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0016 https://security.paloaltonetworks.com/CVE-2022-0017 https://security.paloaltonetworks.com/CVE-2022-0020 https://security.paloaltonetworks.com/CVE-2022-0011 https://security.paloaltonetworks.com/CVE-2022-0018 https://security.paloaltonetworks.com/CVE-2022-0019 https://security.paloaltonetworks.com/CVE-2022-0021

Affected Product	Zimbra
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-4104, CVE-2022-23307, CVE-2022-23305, CVE-2022-23302)
Description	Zimbra has released Security Updates addressing for multiple vulnerabilities. **CVE-2021-4104** - This RedHat vulnerability does not affect the current Supported Zimbra Collaboration Server versions (8.8.15 & 9.0.0). For this vulnerability to affect the server, it needs JMSAppender and the ability to append configuration files. Zimbra does not use the JMSAppender. **CVE-2022-23307** - Zimbra is vulnerable but is not exploitable. To be exploited the system must be running Chainsaw. It is included but is never running. **CVE-2022-23305** - Zimbra is not vulnerable to this vulnerability, since it does not run the JDBCAppender. **CVE-2022-23302** - Zimbra is not vulnerable to this vulnerability, since it does not run the JMSSink.
Affected Products	Zimbra 8.8.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P30#Security_Hotfix_Alert

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.