Advisory Alert

Alert Number: AAA20240517 **Date:** May 17, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware Broadcom	**Critical**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ivanti	**Medium**	Multiple Vulnerabilities
F5	**Medium**	NULL pointer Dereference Vulnerability
OpenSSL	**Low**	Denial of Service Vulnerability
Palo Alto	**Low**	Security Updates

Description

Affected Product	**VMware Broadcom**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22267, CVE-2024-22268, CVE-2024-22269, CVE-2024-22270)
Description	VMware Broadcom has issued security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-22267** - VMware Workstation and Fusion contain a use-after-free vulnerability in the vbluetooth device. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE-2024-22268** - VMware Workstation and Fusion contain a heap buffer-overflow vulnerability in the Shader functionality. A malicious actor with non-administrative access to a virtual machine with 3D graphics enabled may be able to exploit this vulnerability to create a denial of service condition. **CVE-2024-22269** - VMware Workstation and Fusion contain an information disclosure vulnerability in the vbluetooth device. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine. **CVE-2024-22270** - VMware Workstation and Fusion contain an information disclosure vulnerability in the Host Guest File Sharing (HGFS) functionality. A malicious actor with local administrative privileges on a virtual machine may be able to read privileged information contained in hypervisor memory from a virtual machine. VMware Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Workstation 17.x VMware Fusion 13.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24280

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of service and Sensitive information disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 23.10 Ubuntu 22.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6774-1 • https://ubuntu.com/security/notices/USN-6766-2

Affected Product	**Ivanti**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46806, CVE-2023-46807, CVE-2024-22026)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could cause SQL injection and Local Privilege escalation. **CVE-2023-46806** - An SQL Injection vulnerability in a web component of EPMM versions before 12.1.0.0 allows an authenticated user with appropriate privilege to access or modify data in the underlying database. **CVE-2023-46807** - An SQL Injection vulnerability in web component of EPMM before 12.1.0.0 allows an authenticated user with appropriate privilege to access or modify data in the underlying database. **CVE-2024-22026** - A local privilege escalation vulnerability in EPMM before 12.1.0.0 allows an authenticated local user to bypass shell restriction and execute arbitrary commands on the appliance. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Mobile (Core) before 12.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-EPMM-May-2024?language=en_US

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	NULL pointer Dereference Vulnerability (CVE-2023-28484)
Description	F5 has released security updates addressing a NULL pointer Dereference Vulnerability that exists in their products. This vulnerability allows a remote, authenticated (unauthenticated in the case of F5OS and Traffix) attacker to cause a segmentation fault that can lead to a denial-of-service (DoS) on the affected F5 products. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC 5.2.0, 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000139641

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-4603)
Description	OpenSSL has released security updates addressing a Denial of service vulnerability that exists in applications which use the functions EVP_PKEY_param_check() or EVP_PKEY_public_check() to check a DSA public key or DSA parameters. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL 3.3, 3.2, 3.1 and 3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20240516.txt

Affected Product	**Palo Alto**
Severity	**Low**
Affected Vulnerability	Security Updates (CVE-2024-3661)
Description	Palo Alto has released security updates addressing the TunnelVision vulnerability. This issue allows an attacker with the ability to send DHCP messages on the same local area network, such as a rogue Wi-Fi network, to leak traffic outside of the GlobalProtect tunnel, allowing the attacker to read, disrupt, or possibly modify network traffic that was expected to be protected by the GlobalProtect tunnel. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GlobalProtect app on iOS - All versions without IncludeAllNetworks set to 1 GlobalProtect app on Windows and macOS - All versions without Endpoint Traffic Policy Enforcement set to All Traffic
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-3661

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.