TLP: WHITE

Advisory Alert

Alert No: AAA190213 Date: 13-Feb-19 14:04 PM

Classification The Alert : Public Circulation Permitted

Security Updates for 13th February 2019

Overview	High	Microsoft	▪ Multiple Vulnerabilities
		Containers	▪ runC Container Vulnerability
		phpMyAdmin	▪ SQL Injection Attack Vulnerability
	Medium	Adobe Acrobat	▪ Arbitrary Code Execution
		Node.js	▪ Decompress Module Directory Traversal

Description / Impact

Microsoft	• Microsoft has released updates to address multiple vulnerabilities in Microsoft software. Most severe vulnerability could allow for code execution • Affected Products: Windows, Windows Server, Microsoft Office and Multiple Products • Officially Acknowledged by the Vendor: Yes
Containers	• This vulnerability allows an infected container to overwrite the host runC binary and gain root-level code access on the host. • Affected Products: Docker, Kubernetes, ContainerD RunC patch is issued mainly by following platforms: ◦ Red Hat Enterprise Linux 7 ◦ Red Hat OpenShift Container Platform 3.x ◦ Debian ◦ Ubuntu ◦ Amazon Linux • Officially Acknowledged by the Vendor: Yes
phpMyAdmin	• A specially crafted username could be used to exploit a SQL Injection flaw through the designer feature. • Affected Products: Versions 4.5.0 through to version 4.8.4 • Officially Acknowledged by the Vendor: Yes
Adobe Acrobat	• Multiple vulnerabilities have been discovered in Adobe Acrobat and Adobe Reader. • Affected Products: Acrobat DC, Acrobat Reader DC • Officially Acknowledged by the Vendor: Yes
Node.js	• A vulnerability in the "decompress-zip module of Node.js allows an attacker to write arbitrary files when a malicious file is extracted. • Affected Products: Versions before 0.2.2, versions from 0.3.0 and before version 0.3.2 • Officially Acknowledged by the Vendor: Yes

Risk Reduction Recommendations

Visit the links below and follow the instructions given by respective vendors.

Microsoft	• https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/51503ac5-e6d2-e811-a983-000d3a33c573
Container	• https://access.redhat.com/security/cve/cve-2019-5736 • https://access.redhat.com/security/vulnerabilities/runcescape • https://aws.amazon.com/security/security-bulletins/AWS-2019-002/ • https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5736 • https://docs.docker.com/engine/release-notes/ • https://kubernetes.io/blog/2019/02/11/runc-and-cve-2019-5736/ • https://security-tracker.debian.org/tracker/CVE-2019-5736 • https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-5736.html
phpMyAmin	• https://www.phpmyadmin.net/security/PMASA-2019-2/
Adobe	• https://helpx.adobe.com/security/products/acrobat/apsb19-07.html
Node.js	• https://github.com/nodejs/security-wg/blob/master/vuln/npm/488.json

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.