الجمهوريــة الجـزائريـة الديمـقراطيـة الشـعبية
وزارة التعليم العالي والبحث العلمي

مديرية الشبكات وأنظمة الإعلام
والاتصال الجامعية

المديرية الفرعية للأمن المعلوماتي

Courrier électronique: sdsi@mesrs.dz
Site web: www.mesrs.dz

المرجع : DRSICU/SDSI/19/34
الجزائر Alger le 04/07/2019

NOTICE DE SECURITE N° 11/2019 du 04 juillet 2019

A Messieurs les Présidents des Conférences Régionales
A Mesdames et Messieurs les Chefs d'établissement

Objet : Failles de sécurité critiques dans Apache Tomcat, Oracle WebLogic, noyau Linux de SUSE et d'Ubuntu ; Serveur DNS BIND, VideoLAN VLC, F5 BIG-IP, produits Palo Alto, Cisco Data Center Network Manager, VMware Tools et Workstation, Tenable Nessus, Samba, Xen, Citrix.

J'ai l'honneur de vous faire part de la notice de sécurité établie à la suite de la découverte de multiples vulnérabilités critiques dans ***Apache Tomcat, Oracle WebLogic, noyau Linux de SUSE et d'Ubuntu ; Serveur DNS BIND, VideoLAN VLC, F5 BIG-IP, produits Palo Alto, Cisco Data Center Network Manager, VMware Tools et Workstation, Tenable Nessus, Samba, Xen, Citrix..***

I. Apache Tomcat:

Les versions :

- Apache Tomcat 9.0.0.M1 à 9.0.19
- Apache Tomcat 8.5.0 à 8.5.40

sont affectées.

1. RISQUES :

- Déni de service à distance.

2. CORRECTION - PARADE:

Mettre à jour vers les versions stables.

3. SOURCES:

Apache :

http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.20

II. Oracle WebLogic:

Les versions Oracle WebLogic Server 10.3.6.0.0, 12.1.3.0.0 et 12.2.1.3.0 sont affectées.

1. RISQUES :

- Exécution de code arbitraire.

2. CORRECTION - PARADE:

Mettre à jour vers les versions stables.

3. SOURCES:

Oracle:
https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2729-5570780.html

III. Noyau Linux de SUSE:

Les versions :

- SUSE Linux Enterprise Live Patching 12-SP3
- SUSE Linux Enterprise Live Patching 12-SP4
- SUSE Linux Enterprise Server 12-LTSS
- SUSE Linux Enterprise Server 12-SP1-LTSS
- SUSE Linux Enterprise Server 12-SP2-LTSS
- SUSE Linux Enterprise Server for SAP 12-SP1
- SUSE Linux Enterprise Server for SAP 12-SP2
- SUSE Linux Enterprise Module for Public Cloud 12

sont affectées.

1. RISQUES :

- Déni de service,
- Atteinte à la confidentialité des données,
- Élévation de privilèges.

2. CORRECTION - PARADE:

Installez les correctifs de sécurité disponibles sur les liens ci-dessous:

3. SOURCES:

SUSE:

https://www.suse.com/support/update/announcement/2019/suse-su-20191668-1/

https://www.suse.com/support/update/announcement/2019/suse-su-20191671-1/

https://www.suse.com/support/update/announcement/2019/suse-su-20191674-1/

https://www.suse.com/support/update/announcement/2019/suse-su-20191692-1/

IV. Noyau Linux d'Ubuntu:

Les versions :

- Ubuntu 19.04
- Ubuntu 18.10
- Ubuntu 18.04 LTS
- Ubuntu 16.04 LTS
- Ubuntu 14.04 ESM

sont affectées.

1. RISQUES :

- Déni de service,
- Atteinte à l'intégrité des données,
- Atteinte à la confidentialité des données.

2. CORRECTION - PARADE:

Installez les correctifs de sécurité disponibles sur les liens ci-dessous:

3. SOURCES:

Ubuntu:

https://usn.ubuntu.com/4041-1/

https://usn.ubuntu.com/4041-2/

https://usn.ubuntu.com/4031-1/

V. Serveur DNS BIND:

Les versions :

- BIND 9.11.0 à 9.11.7, 9.12.0 à 9.12.4-P1 et 9.14.0 à 9.14.2
- Toutes les versions BIND 9.13 et 9.15
- BIND Supported Preview Edition 9.11.3-S1 à 9.11.7-S1

sont affectées.

1. RISQUES :

- Déni de service.

2. CORRECTION - PARADE:

Mettre à jour vers les versions stables.

3. SOURCES:

BIND:

https://kb.isc.org/docs/cve-2019-6471

VI. VideoLAN VLC:

Toutes les versions VLC media player antérieures à 3.0.7 sont affectées

1. RISQUES :

- Déni de service,
- Exécution de code arbitraire à distance.

2. CORRECTION - PARADE:

Mettre à jour vers la version 3.0.7.

3. SOURCES:

VideoLAN:

https://www.videolan.org/security/sa1901.html

VII. F5 BIG-IP:

Toutes les versions BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator, WebSafe) antérieures à 15.0.0 sont affectées.

1. RISQUES :

- Contournement de la fonctionnalité de sécurité,
- Atteinte à la confidentialité des données,
- Élévation de privilèges,
- Déni de service.

2. CORRECTION - PARADE:

Mettre à jour vers la version 15.0.0.

3. SOURCES:

f5 :

https://support.f5.com/csp/article/K54252492

https://support.f5.com/csp/article/K20934447

https://support.f5.com/csp/article/K00040234

https://support.f5.com/csp/article/K25244852

https://support.f5.com/csp/article/K21462542

https://support.f5.com/csp/article/K24401914

https://support.f5.com/csp/article/K74374841

https://support.f5.com/csp/article/K95275140

https://support.f5.com/csp/article/K31300402

https://support.f5.com/csp/article/K49711130

https://support.f5.com/csp/article/K01713115

https://support.f5.com/csp/article/K87659521

https://support.f5.com/csp/article/K38941195

https://support.f5.com/csp/article/K82814400

VIII. Produits Palo Alto:

Les versions :

- PAN-OS antérieures à 7.1.24
- PAN-OS 8.0.x antérieures à 8.0.19
- PAN-OS 8.1.x antérieures à 8.1.8-h5
- PAN-OS 9.0.x antérieures à 9.0.2-h4
- Traps antérieures à 5.0.5
- MineMeld antérieures à 0.9.62

sont affectées.

1. RISQUES :

- Exécution de code arbitraire à distance,
- Déni de service à distance,
- Injection de code indirecte à distance (XSS).

2. CORRECTION - PARADE:

Mettre à jour vers les versions stables.

3. SOURCES:

Palo Alto:

https://securityadvisories.paloaltonetworks.com/Home/Detail/151

https://securityadvisories.paloaltonetworks.com/Home/Detail/152

https://securityadvisories.paloaltonetworks.com/Home/Detail/153

IX. Cisco Data Center Network Manager:

Toutes les versions Cisco Data Center Network Manager (DCNM) antérieures à 11.2(1) sont affectées.

1. RISQUES :

- Exécution de code arbitraire,
- Contournement de la politique de sécurité,
- Atteinte à l'intégrité des données.

2. CORRECTION - PARADE:

Mettre à jour vers la version 11.2(1).

3. SOURCES:

Cisco :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-codex

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-bypass

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190626-dcnm-file-dwnld

X. Produits VMware:

Les produits :

- AppDefense
- Container Service Extension
- Enterprise PKS
- Horizon
- Horizon DaaS
- Hybrid Cloud Extension
- Identity Manager
- Integrated OpenStack
- NSX for vSphere
- NSX-T Data Center
- Pulse Console
- SD-WAN Edge by VeloCloud
- SD-WAN Gateway by VeloCloud
- SD-WAN Orchestrator by VeloCloud
- Skyline Collector
- Unified Access Gateway
- vCenter Server Appliance
- vCloud Availability Appliance
- vCloud Director For Service Providers
- vCloud Usage Meter
- vRealize Automation
- vRealize Business for Cloud
- vRealize Code Stream
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations Manager
- vRealize Orchestrator Appliance
- vRealize Suite Lifecycle Manager
- vSphere Data Protection
- vSphere Integrated Containers
- vSphere Replicatio

sont affectées.

1. RISQUES :

- Exécution de code arbitraire à distance.

2. CORRECTION - PARADE:

Mettre à jour vers les versions stables.

3. SOURCES:

VMware:

https://www.vmware.com/security/advisories/VMSA-2019-0010.html

XI. Tenable Nessus:

Toutes les versions Nessus antérieures à 8.5.0 sont affectées.

1. RISQUES :

- Atteinte à la confidentialité des données,
- Déni de service.

2. CORRECTION - PARADE:

Mettre à jour vers la version 8.5.0.

3. SOURCES:

Tenable:
https://www.tenable.com/security/tns-2019-04

XII. Samba:

Les versions :

- Samba 4.10 antérieures à 4.10.5
- Samba 4.9 antérieures à 4.9.9

sont affectées.

1. RISQUES :

- Déni de service.

2. CORRECTION - PARADE:

Mettre à jour vers les versions stables.

3. SOURCES:

Samba :

https://www.samba.org/samba/security/CVE-2019-12435.html

https://www.samba.org/samba/security/CVE-2019-12436.html

XIII. Xen:

Toutes les versions Xen sans les derniers correctifs de sécurité sont affectées.

1. RISQUES :

- Déni de service.

2. CORRECTION - PARADE:

Installez les correctifs de sécurité disponibles sur le lien ci-dessous:

3. SOURCES:

Xen:

https://xenbits.xen.org/xsa/advisory-295.html

XIV. Citrix:

Toutes les versions AppDNA antérieures à 7 1906.1.0.472 sont affectées.

1. RISQUES :

- Exécution de code arbitraire à distance,
- Élévation de privilèges.

2. CORRECTION - PARADE:

Mettre à jour vers la version 7 1906.1.0.472.

3. SOURCES:

Citrix:

https://support.citrix.com/article/CTX253828

DIFFUSION: La sécurité est l'affaire de tous, dans l'intérêt de tout le monde, merci d'assurer la diffusion de ces informations la plus large entre et dans les établissements.

Salutations cordiales.