Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 19 avril 2017
N° CERTFR-2017-AVI-120

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Oracle Sun Systems Products Suite

Gestion du document

Référence	CERTFR-2017-AVI-120
Titre	Multiples vulnérabilités dans Oracle Sun Systems Products Suite
Date de la première version	19 avril 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle cpuapr2017-3236618 du 18 avril 2017 Bulletin de sécurité Oracle cpuapr2017verbose-3236619 du 18 avril 2017
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- exécution de code arbitraire à distance
- déni de service à distance
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Oracle Solaris Cluster version 4.3
- Oracle StorageTek Tape Analytics SW Tool versions antérieures à 2.2.1
- Oracle Sun ZFS Storage Appliance Kit (AK) version AK 2013
- Oracle SuperCluster Specific Software version 2.3.8
- Oracle SuperCluster Specific Software version 2.3.13
- Oracle Solaris version 11.3
- Oracle Solaris version 10

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Oracle Sun Systems Products Suite*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à l'intégrité des données.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Oracle cpuapr2017-3236618 du 18 avril 2017
  http://www.oracle.com/technetwork/security-advisory/cpuapr2017-3236618.html
- Bulletin de sécurité Oracle cpuapr2017verbose-3236619 du 18 avril 2017
  http://www.oracle.com/technetwork/security-advisory/cpuapr2017verbose-3236619.html#SUNS
- Référence CVE CVE-2015-4852
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4852
- Référence CVE CVE-2015-7501
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7501
- Référence CVE CVE-2016-3607
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3607
- Référence CVE CVE-2016-5019
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5019
- Référence CVE CVE-2016-5551
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5551
- Référence CVE CVE-2017-3474
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3474
- Référence CVE CVE-2017-3497
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3497
- Référence CVE CVE-2017-3498
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3498
- Référence CVE CVE-2017-3510
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3510
- Référence CVE CVE-2017-3516
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3516
- Référence CVE CVE-2017-3551
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3551
- Référence CVE CVE-2017-3564
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3564
- Référence CVE CVE-2017-3565
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3565
- Référence CVE CVE-2017-3578
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3578
- Référence CVE CVE-2017-3580
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3580
- Référence CVE CVE-2017-3582
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3582
- Référence CVE CVE-2017-3584
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3584
- Référence CVE CVE-2017-3585
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3585

- Référence CVE CVE-2017-3621
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3621
- Référence CVE CVE-2017-3622
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3622
- Référence CVE CVE-2017-3623
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3623

Gestion détaillée du document

19 avril 2017 version initiale.