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 20 juillet 2016
N° CERTFR-2016-AVI-244

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Oracle Sun Systems Products Suite

Gestion du document

Référence	CERTFR-2016-AVI-244
Titre	Multiples vulnérabilités dans Oracle Sun Systems Products Suite
Date de la première version	20 juillet 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle cpujul2016-2881720 du 19 juillet 2016
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)

- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Oracle Integrated Lights Out Manager (ILOM) versions 3.0, 3.1 et 3.2
- Commutateurs Sun Data Center InfiniBand versions antérieures à 2.2.2
- Commutateurs de Passerelle Sun Network QDR InfiniBand versions antérieures à 2.2.2
- Serveurs SPARC Enterprise M3000, M4000, M5000, M8000, M9000 exécutant XCP versions antérieures à XCP1121
- Commutateurs Ethernet 40G 10G 72/64 version 2.0.0
- Commutateurs Oracle ES1-24 version 1.3
- Sun Blade 6000 Ethernet Switched NEM 24P 10GE version 1.2
- Commutateurs Sun Network 10GE 72p version 1.2
- Oracle Solaris versions 10 et 11.3
- Serveurs Fujitsu M10-1, M10-4, M10-4S exécutant XCP versions antérieures à XCP2320
- Oracle Solaris Cluster versions 3.4 et 4.3

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Oracle Sun Systems Products Suite*. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité 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 cpujul2016-2881720 du 19 juillet 2016
  http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
- Bulletin de sécurité Oracle cpujul2016verbose-2881721 du 19 juillet 2016
  http://www.oracle.com/technetwork/security-advisory/cpujul2016verbose-2881721.html#SUNS
- Référence CVE CVE-2012-3410
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-3410
- Référence CVE CVE-2013-2566
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2566
- Référence CVE CVE-2014-3566
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
- Référence CVE CVE-2015-0235
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235
- Référence CVE CVE-2015-1793
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1793
- Référence CVE CVE-2015-2808
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2808
- Référence CVE CVE-2015-3183
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3183
- Référence CVE CVE-2015-3197
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3197
- Référence CVE CVE-2015-5600
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5600
- Référence CVE CVE-2015-8104
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8104
- Référence CVE CVE-2016-0800
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
- Référence CVE CVE-2016-3451
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3451
- Référence CVE CVE-2016-3453
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3453
- Référence CVE CVE-2016-3480
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3480
- Référence CVE CVE-2016-3481
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3481
- Référence CVE CVE-2016-3497
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3497
- Référence CVE CVE-2016-3584
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3584
- Référence CVE CVE-2016-3585
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3585
- Référence CVE CVE-2016-5445
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5445

- Référence CVE CVE-2016-5446
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5446
- Référence CVE CVE-2016-5447
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5447
- Référence CVE CVE-2016-5448
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5448
- Référence CVE CVE-2016-5449
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5449
- Référence CVE CVE-2016-5452
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5452
- Référence CVE CVE-2016-5453
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5453
- Référence CVE CVE-2016-5454
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5454
- Référence CVE CVE-2016-5457
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5457
- Référence CVE CVE-2016-5469
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5469
- Référence CVE CVE-2016-5471
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5471

Gestion détaillée du document

20 juillet 2016 version initiale.