

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Oracle Sun Systems

Gestion du document

Référence	CERTFR-2015-AVI-306
Titre	Multiples vulnérabilités dans Oracle Sun Systems
Date de la première version	15 juillet 2015
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle du 14 juillet 2015
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)

- non spécifié par l'éditeur

2 - Systèmes affectés

- ILOM versions 3.2.6 et antérieures
- Oracle Ethernet Switch ES2-72 versions 1.9.1.2 et antérieures
- Oracle Ethernet Switch ES2-64 versions 1.9.1.2 et antérieures
- Oracle Switch ES1-24 versions 1.3.1 et antérieures
- Sun Blade 6000 Ethernet Switched NEM 24P 10GE versions 1.2.2 et antérieures
- Sun Network 10GE Switch 72p versions 1.2.2 et antérieures
- Fujitsu M10-1 versions XCP 2260 et antérieures
- Fujitsu M10-4 versions XCP 2260 et antérieures
- Fujitsu M10-4S servers versions XCP 2260 et antérieures
- SPARC Enterprise M3000 versions XCP 1120 et antérieures
- SPARC Enterprise M4000 versions XCP 1120 et antérieures
- SPARC Enterprise M5000 versions XCP 1120 et antérieures
- SPARC Enterprise M8000 versions XCP 1120 et antérieures
- SPARC Enterprise M9000 versions XCP 1120 et antérieures
- Solaris versions 10 et antérieures
- Solaris versions 11.2 et antérieures

- Solaris Cluster versions 3.3 et antérieures
- Solaris Cluster versions 4.2 et antérieures
- Oracle VM Server for SPARC versions 3.2 et antérieures

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Oracle Sun Systems*. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.

4 - Contournement provisoire

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

5 - Documentation

- Bulletin de sécurité Oracle du 14 juillet 2015
<http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html>
- Référence CVE CVE-2015-0235
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0235>
- Référence CVE CVE-2015-2580
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2580>
- Référence CVE CVE-2015-2589
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2589>
- Référence CVE CVE-2015-2609
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2609>
- Référence CVE CVE-2015-2614
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2614>
- Référence CVE CVE-2015-2616
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2616>
- Référence CVE CVE-2015-2631
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2631>
- Référence CVE CVE-2015-2651
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2651>
- Référence CVE CVE-2015-2662
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2662>
- Référence CVE CVE-2015-4750
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4750>
- Référence CVE CVE-2015-4770
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4770>
- Référence CVE CVE-2014-3571
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3571>
- Référence CVE CVE-2013-5704
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5704>
- Référence CVE CVE-2014-3570
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3570>

Gestion détaillée du document

15 juillet 2015 version initiale.