



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 20 avril 2011
N° CERTA-2011-AVI-239

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités dans les produits Oracle Sun

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-239>

Gestion du document

Référence	CERTA-2011-AVI-239
Titre	Multiples Vulnérabilités dans les produits Oracle Sun
Date de la première version	20 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Oracle d'avril 2011
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Oracle Sun Solaris versions 8, 9, 10, 11 Express;
- Oracle Sun Glassfish Enterprise Server, Oracle Sun Java System Application Server versions 2.1, 2.11, 3.0.1, 9.1;
- Oracle Sun Java System Messaging Server versions 6.3, 7.0;
- Oracle iplanet Web Server (Sun Java System Web Server) versions 6.1, 7.0;
- Oracle Sun Java System Access Manager Policy Agent version 2.2;
- Oracle Java Dynamic Management Kit version 5.1;
- Oracle Open SSO Enterprise, Sun Java system Access Manager versions 7.1, 8.0.

3 Résumé

De multiples vulnérabilités présentes dans les produits Oracle Sun ont été corrigées.

4 Description

De multiples vulnérabilités présentes dans les produits Oracle Sun ont été corrigées. Les détails de ces vulnérabilités n'ont pas été divulgués mais l'une d'entre elles à un niveau de criticité maximal dans l'échelle de l'éditeur (10).

5 Solution

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

6 Documentation

- Bulletin de sécurité Oracle d'avril 2011 :
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2011-301950.html>
- Référence CVE CVE-2011-0807 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0807>
- Référence CVE CVE-2011-0841 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0841>
- Référence CVE CVE-2011-0800 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0800>
- Référence CVE CVE-2011-0411 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0411>
- Référence CVE CVE-2011-0820 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0820>
- Référence CVE CVE-2010-4476 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4476>
- Référence CVE CVE-2011-0846 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0846>
- Référence CVE CVE-2011-0813 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0813>
- Référence CVE CVE-2011-0829 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0829>
- Référence CVE CVE-2011-0849 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0849>
- Référence CVE CVE-2011-0847 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0847>
- Référence CVE CVE-2011-0844 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0844>
- Référence CVE CVE-2011-0812 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0812>
- Référence CVE CVE-2011-0839 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0839>
- Référence CVE CVE-2011-0821 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0821>
- Référence CVE CVE-2011-0801 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0801>
- Référence CVE CVE-2011-0790 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0790>

Gestion détaillée du document

20 avril 2011 version initiale.