



# multiples vulnérabilités dans Apple iTunes | Le Net Expert Informatique

|   |   |
|---|---|
|  <p>Le Net Expert<br/><b>INFORMATIQUE</b><br/>Protection des données personnelles<br/>Sécurité Informatique - Cybercriminalité</p>  <p><b>vous informe...</b></p> | <p><b> multiples vulnérabilités<br/>dans Apple iTunes</b></p> |
|---|---|

1 - Risque(s)exécution de code arbitraire à distance  
dédi de service à distance  
atteinte à la confidentialité des données

2 - Systèmes affectés  
Apple iTunes version antérieure à 12.3

3 - Résumé  
De multiples vulnérabilités ont été corrigées dans Apple iTunes. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité 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 Apple HT205221 du 16 septembre 2015  
<https://support.apple.com/fr-fr/HT205221>

Référence CVE CVE-2010-3199  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3199>  
Référence CVE CVE-2014-8146  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8146>  
Référence CVE CVE-2015-1152  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1152>  
Référence CVE CVE-2015-1153  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1153>  
Référence CVE CVE-2015-1157  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1157>  
Référence CVE CVE-2015-1205  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1205>  
Référence CVE CVE-2015-3686  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3686>  
Référence CVE CVE-2015-3687  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3687>  
Référence CVE CVE-2015-3688  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3688>  
Référence CVE CVE-2015-3730  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3730>  
Référence CVE CVE-2015-3731  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3731>  
Référence CVE CVE-2015-3732  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3732>  
Référence CVE CVE-2015-3733  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3733>  
Référence CVE CVE-2015-3734  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3734>  
Référence CVE CVE-2015-3735  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3735>  
Référence CVE CVE-2015-3736  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3736>  
Référence CVE CVE-2015-3737  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3737>  
Référence CVE CVE-2015-3738  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3738>  
Référence CVE CVE-2015-3739  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3739>  
Référence CVE CVE-2015-3740  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3740>  
Référence CVE CVE-2015-3741  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3741>  
Référence CVE CVE-2015-3742  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3742>  
Référence CVE CVE-2015-3743  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3743>  
Référence CVE CVE-2015-3744  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3744>  
Référence CVE CVE-2015-3745  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3745>  
Référence CVE CVE-2015-3746  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3746>  
Référence CVE CVE-2015-3747  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3747>  
Référence CVE CVE-2015-3748  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3748>  
Référence CVE CVE-2015-3749  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3749>  
Référence CVE CVE-2015-3755  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3755>  
Référence CVE CVE-2015-5761  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5761>  
Référence CVE CVE-2015-5769  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5769>  
Référence CVE CVE-2015-5790  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5790>  
Référence CVE CVE-2015-5791  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5791>  
Référence CVE CVE-2015-5792  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5792>  
Référence CVE CVE-2015-5793  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5793>  
Référence CVE CVE-2015-5794  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5794>  
Référence CVE CVE-2015-5795  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5795>  
Référence CVE CVE-2015-5796  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5796>  
Référence CVE CVE-2015-5797  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5797>  
Référence CVE CVE-2015-5798  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5798>  
Référence CVE CVE-2015-5799  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5799>  
Référence CVE CVE-2015-5800  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5800>  
Référence CVE CVE-2015-5801  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5801>  
Référence CVE CVE-2015-5802  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5802>  
Référence CVE CVE-2015-5803  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5803>  
Référence CVE CVE-2015-5804  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5804>  
Référence CVE CVE-2015-5805  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5805>  
Référence CVE CVE-2015-5806  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5806>  
Référence CVE CVE-2015-5807  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5807>  
Référence CVE CVE-2015-5808  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5808>  
Référence CVE CVE-2015-5809  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5809>  
Référence CVE CVE-2015-5810  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5810>  
Référence CVE CVE-2015-5811  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5811>  
Référence CVE CVE-2015-5812  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5812>  
Référence CVE CVE-2015-5813  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5813>  
Référence CVE CVE-2015-5814  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5814>  
Référence CVE CVE-2015-5815  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5815>  
Référence CVE CVE-2015-5816  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5816>  
Référence CVE CVE-2015-5817  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5817>  
Référence CVE CVE-2015-5818  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5818>  
Référence CVE CVE-2015-5819  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5819>  
Référence CVE CVE-2015-5821  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5821>  
Référence CVE CVE-2015-5822  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5822>  
Référence CVE CVE-2015-5823  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5823>  
Référence CVE CVE-2015-5874  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5874>  
Référence CVE CVE-2015-5920  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-5920>

Gestion détaillée du document  
18 septembre 2015  
version initiale  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2015-AVI-398>

Même si remplir un formulaire de déclaration à la CNIL est gratuit et enfantin, il vous engage cependant, par la signature que vous apposez, à respecter scrupuleusement la loi Informatique et Libertés. Cette démarche doit d'abord commencer par un Audit de l'ensemble de vos systèmes de traitements de données. Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybersécurité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?  
Contactez-nous  
Denis JACOPINI  
Tel : 06 10 71 79 12  
formatteur n°93 84 93041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.  
Nos domaines de compétence :  
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet ;  
• **Consultant en sécurité informatique**, cybersécurité et mises en conformité et déclarations à la CNIL ;  
• **Formateur et chargé de cours** en sécurité informatique, cybersécurité et déclarations à la CNIL.  
Contactez-nous

Cet article vous plaît ? Partagez !  
Un avis ? Laissez-nous un commentaire !

Source : <http://www.cert.ssi.gouv.fr/site/CERTFR-2015-AVI-398/CERTFR-2015-AVI-398.html>