Avis de vulnérabilité
Advisory

ISEC-V2011-01-v-1.1

UCOPIA COMMUNICATIONS
Interface de management
Contournement de l'authentification

Notre métier : préserver le vôtre.

WWW.INTRINSEC.COM
215 AV G. CLEMENCEAU 92024 NANTERRE ● TÉL +33 1 41 91 77 77 ● FAX +33 1 41 91 77 78
SAS AU CAPITAL DE 480 000 € ● SIREN 402 336 085 ● TVA FR 19 402 336 085 ● APE 721Z

1 AVIS ISEC-V2011-01-v-1.1

Éditeur : **UCOPIA COMMUNICATIONS**

Produit : **UCOPIA Express**

Titre : **Contournement d'authentification - interface d'administration**

Identifiant Intrinsec : **ISEC-V2011-01-v-1.1**

Date de publication : **1er Juillet 2011**

Date de dernière mise à jour : **1er Juillet 2011**

Niveau de risque : **Élevé**

Exploitable : **À distance**

Impact :

- Contournement d'une mesure de sécurité
- Manipulation de données
- Exposition de données sensibles
- Élévation de privilèges
- Déni de service

Description :

Un problème d'implémentation du processus d'authentification sur l'interface d'administration du portail captif UCOPIA permet son contournement et l'obtention des privilèges d'administration de la solution.

Versions concernées :

Contrôleur UCOPIA Express 50 Version 4.1 (build : 10060105)

Solutions : Mettre à jour en version 4.1 build 10060107 ou plus récent

Références :

Aucunes

Crédit :

Vulnérabilité découverte par Olivier Cassignac (olivier.cassignac@intrinsec.com) et Loïc Michaux (loic.michaux@intrinsec.com).

Vulnérabilité divulguée en concertation avec l'éditeur et le CERT-IST.

Historique :

2011-06-29: Découverte de la vulnérabilité

2011-07-04: Notification du CERT-IST

2011-09-26: Ucopia communique sur la correction de la vulnérabilité

2 ADVISORY ISEC-V2011-01-v-1.1

Editor: **UCOPIA COMMUNICATIONS**

Product: **UCOPIA Express**

Title: **Management interface – authentication bypass**

Intrinsec ID: **ISEC-V2011-01-v-1.1**

Publication date: **July 1st 2011**

Last update: **July 1st 2011**

Risk level: **High**

Exploitable: **Remotely**

Impact:

- Security function bypass
- Data manipulation
- Sensitive data exposure
- Privilege escalation
- Denial of service

Description:

An implementation issue in the administration interface authentication process of the UCOPIA captive portal allows bypassing authentication then gain administrative privileges of the solution.

Versions affected:

Controller UCOPIA Express 50 Version 4.1 (build : 10060105)

Solutions: Update to version 4.1 build 10060107 or newer

References:

None

Credits:

Vulnerability discovered Olivier Cassignac (olivier.cassignac@intrinsec.com) and Loïc Michaux (loic.michaux@intrinsec.com)

Vulnerability disclosed in coordination with the constructor and the CERT-IST

History:

2011-06-29: Vulnerability discovery

2011-07-04: CERT-IST Notification

2011-09-26: Ucopia communicates on fixing the vulnerability