

# 天津市工业和信息化委员会

---

## 市工业和信息化委关于转发金雅拓产品存在网络安全高危漏洞风险通报的通知

各区工业和信息化主管部门,工业集团公司,有关单位:

日前,我委接到国家工业信息安全发展研究中心发来的关于金雅拓产品存在网络安全高危漏洞的风险通报。我国大量在用的工业控制系统包括亚控、力控、西门子、ABB、通用电气等产品及部分信息系统均采用该软件许可服务并受到漏洞影响,影响范围非常广泛。为了提高重视,加强防范,现将风险通报转发给你们,请你单位做好风险通报、应急处置等工作,发现类似安全问题及时与我委进行沟通。

附件:关于金雅拓产品存在网络安全高危漏洞的风险通报



(联系人:市工业和信息化委工业信息安全处 董津;  
联系电话(传真):23306557;  
电子邮箱:dongjin1979@126.com)

# 国家工业信息安全发展研究中心

---

## 关于金雅拓产品存在网络安全高危漏洞 的风险通报

2018年1月23日，卡巴斯基公司（Kaspersky）在其官网发布研究报告披露多款金雅拓 Safenet 软件许可服务产品存在 14 个安全漏洞（其中有 8 个得到证实，漏洞细节见附件），受影响的为使用 Sentinel LDK RTE 7.6 运行环境（含之前版本在内）的 HASP SRM、Sentinel HASP、Sentinel LDK 金雅拓 Safenet 产品。我国大量在用的工业控制系统，包括亚控、力控、西门子、ABB、通用电气等产品及部分信息系统均采用该软件许可服务并受到漏洞影响，影响范围非常广泛。现就具体情况通报如下：

### 一、漏洞分析

金雅拓 Safenet 软件许可服务产品广泛应用于工业控制系统和传统 IT 系统。该产品的软件部分包括驱动程序、Web 应用程序和其他软件组件等，硬件部分包括 USB 令牌，USB 令牌在首次连接主机时将自动安装驱动程序并开启 1947 端口。目前，安全研究人员发现金雅拓 Safenet 软件许可服务产品存在 14 个安全漏洞，攻击者通过开启的 1947 端口，可利

---

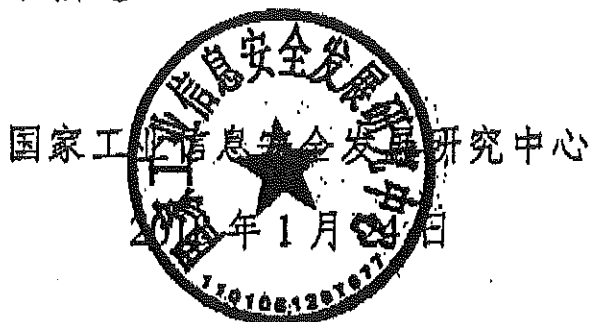
用上述安全漏洞进行拒绝服务（DoS）攻击、中间人攻击和以系统权限执行任意代码等恶意攻击，造成信息泄露、系统崩溃等严重后果。

## 二、对策建议

（一）开展漏洞修复工作。目前，金雅拓官方已经发布补丁对漏洞进行修复，建议工业控制系统厂商及工业控制系统安全企业及时验证补丁可用性；各工业企业做好补丁离线测试和修复工作。

（二）为了防止该漏洞被远程利用，各工业企业按照《工业控制系统信息安全防护指南》要求，开展工业控制系统及工控主机的安全防护工作。一是做好安全配置，定期进行配置审计；二是通过边界防护设备对工控网络与企业网或互联网的边界进行安全防护；三是强化登录账户及密码，避免弱口令；四是关闭不必要的 HTTP、FTP、TELNET 等高风险服务，如无必要，关闭设备的 1947 端口，确需远程访问的，使用虚拟专用网络（VPN）进行接入。

附件：漏洞列表及细节描述



## 附件

## 漏洞列表及细节描述

序号	CVE 编号	漏洞类型	漏洞等级	漏洞概述
1	CVE-2017-11496	远程执行代码漏洞	9.8	金雅拓管理控制中心的 hasplms 服务存在堆栈缓冲区溢出漏洞, 允许远程攻击者通过发送 V2C 格式的畸形 ASN.1 流文件在目标系统执行任意代码。
2	CVE-2017-11497	远程执行代码漏洞	9.8	攻击者发送包含错误格式的文件包, 从而导致堆栈缓冲区溢出, 进而任意代码执行。
3	CVE-2017-11498	拒绝服务漏洞	7.5	远程攻击者可以用无效的 HTML 文件自行创建数据包文件, 导致远程进程拒绝服务。
4	CVE-2017-12818	拒绝服务漏洞	7.5	攻击者可利用 Sentinel HASP 和 Sentinel LDK 产品中的自定义 XML 解析器堆栈溢出导致远程拒绝服务。
5	CVE-2017-12819	NTLM 哈希捕获漏洞	7.3	攻击者利用数据包更新程序, 导致受影响产品中的系统用户受到 NTLM 中继攻击。
6	CVE-2017-12820	拒绝服务漏洞	7.5	攻击者可通过内存指针的任意内存读取功能引发系统远程拒绝服务。
7	CVE-2017-12821	远程执行代码漏洞	9.8	受影响产品中的内存损坏可能会导致攻击者执行远程执行代码操作。
8	CVE-2017-12822	使用配置文件进行远程操作漏洞	9.9	未经身份验证的攻击者可能能够利用漏洞在远程系统上打开新的攻击媒介。