

河南省教育信息安全监测中心
关于大华 DSS 数字监控系统存在 SQL 注入
漏洞的情况通报



河南省教育信息安全监测中心
Henan Provincial Education Information Security Monitoring Center

2024 年 06 月 27 日

关于大华 DSS 数字监控系统存在 SQL 注入漏洞的情况通报

漏洞背景

大华 DSS (Digital Surveillance System) 数字监控系统是一款功能强大的安防视频监控系统，广泛应用于各类安全监控场景。具备实时监视、云台操作、录像回放、报警处理、设备管理等功能，应用比较广泛。

漏洞描述

今年以来，多家单位使用的大华视频监控系统、大华智慧园区综合管理系统遭境外黑客组织攻击渗透。经核实，浙江大华技术股份有限公司研发的大华 DSS 数字监控系统存在 SQL 注入漏洞。

攻击者可以通过向 `attachment_clearTempFile.action` 发送特殊构造的数据包，利用报错注入获取数据库敏感信息。攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限。

漏洞编号

CNNVD-2024-70214332

影响范围

目前已知下列产品受到影响:

受影响产品型号	受影响版本
DH-DSS7016-D DH-DSS7016-DR	V3. 10. 001-V3. 11. 008
DH-DSS-H500	V3. 02. 000-V4. 02. 000 V4. 003. 0000000. 0-V4. 003. 0000001. 0
DH-DSS-H8900	V3. 31. 000-V3. 33. 000 V3. 001. 0000000. 3-V3. 001. 0000004. 15
DH-DSS-N8000	V3. 000. 0000002. 3-V3. 001. 0000004. 1
DH-DSS-C8100	V3. 03. 013-V3. 05. 101
DH-DSS-C700	V3. 01. 82-V3. 01. 114
DH-DSS-T8100	V1. 03. 000-V3. 006. 109

注: 查看版本请登录 Web 界面, 在“关于”页面查看。

安全建议

该系统应用广泛, 并涉及部分高校、党政机关, 请各单位高度重视, 立即组织排查本单位相关产品使用情况, 并采取以下措施及时堵塞安全隐患。同时, 加强网络安全监测, 如发现遭攻击情况及时处置报告。

- 1、限制 attachment_clearTempFile_action 接口的访问;
- 2、联系厂商技术支持人员进行升级修复。



3、关注大华官网，及时获取补丁信息：

<https://www.dahuatech.com/>

联系方式

地址：河南省郑州市二七区大学路 75 号郑州大学南校区逸夫楼西

电话：0371-67761893、0371-67765016

传真：0371-67763770

邮箱：hercert@ha.edu.cn

邮编：450052