# 宏景 e-HR SQL 注入漏洞


2023 年 5 月 12 日

# 一、漏洞概要

| | |
|---|---|
| 漏洞名称 | 宏景 e-HR SQL 注入漏洞 |
| 发布时间 | 2023 年 5 月 12 日 |
| 组件名称 | 宏景 e-HR |
| 影响范围 | 不详 |
| 漏洞类型 | SQL 注入 |
| 利用条件 | 1、用户认证：否<br>2、前置条件：默认配置<br>3、触发方式：远程 |
| 综合评价 | <综合评定利用难度>：容易，无需授权即可利用<br><综合评定威胁等级>:高危,能造成敏感信息泄露。 |
| 官方解决方案 | 已发布 |

# 二、漏洞分析

## 2.1 组件介绍

宏景 e-HR 人力资源管理系统是一款专业的企业级人力资源管理软件，旨在帮助企业实现人力资源信息化管理。该系统包括员工档案管理、招聘管理、培训管理、绩效管理、薪酬管理、考勤管理等多个模块，可以帮助企业实现全面的人力资源管理。

## 2.2 漏洞描述

2023 年 5 月 12 日，深信服安全团队监测到一则宏景 e-HR 组件存在 SQL 注入漏洞的信息，漏洞编号：CNVD-2023-08743，漏洞威胁等级：高危。

该漏洞是由于宏景 e-HR 的某页面的过滤不严谨，导致攻击者可利用该漏洞在未授权的情况下，构造恶意数据执行 SQL 注入攻击，最终造成服务器敏感性信息泄露。

## 三、影响范围

宏景 e-HR 产品是较为流行的人力资源管理系统，属于商业软件，可能受影响的资产主要位于国内。

目前受影响的宏景 e-HR 版本：不详

# 四、解决方案

## 4.1 修复建议

### 1.官方修复建议

当前官方已发布最新版本，建议受影响的用户及时更新升级到最新版本。链接如下：

http://www.hjsoft.com.cn

## 4.2 深信服解决方案

### 1.风险资产发现

支持对宏景 e-HR 的主动检测，可**批量检出**业务场景中该事件的**受影响资产**情况，相关产品如下：

【深信服云镜 YJ】已发布资产检测方案。

### 2.漏洞主动检测

支持对宏景 e-HR SQL 注入漏洞的主动检测，可**批量快速检出**业务场景中是否存在**漏洞风险**，相关产品如下：

【深信服云镜 YJ】预计 2023 年 5 月 12 日发布检测方案。

【深信服漏洞评估工具 TSS】预计 2023 年 5 月 15 日发布检测方案。

【深信服安全托管服务 MSS】预计 2023 年 5 月 12 日发布检测方案。

【深信服安全检测与响应平台 XDR】预计 2023 年 5 月 12 日发布检测方案。

### 3.漏洞安全监测

支持对宏景 e-HR SQL 注入漏洞的监测，可依据流量收集**实时监控**业务场景中的**受影响资产情况，快速检查受影响范围**，相关产品及服务如下：

【深信服安全感知管理平台 SIP】已发布检测方案。

【深信服安全托管服务 MSS】已发布检测方案。

【深信服安全检测与响应平台 XDR】已发布检测方案。

### 4.漏洞安全防护

支持对宏景 e-HR SQL 注入漏洞的防御，**可阻断攻击者针对该事件的入侵行为**，相关产品及服务如下：

【深信服下一代防火墙 AF】已发布防护方案。

【深信服 Web 应用防火墙 WAF】已发布防护方案。

【深信服安全托管服务 MSS】已发布防护方案。

【深信服安全检测与响应平台 XDR】已发布防护方案。

## 五、时间轴

2023/5/12　深信服监测到宏景 e-HR SQL 注入漏洞攻击信息。

2023/5/12　深信服千里目安全技术中心发布漏洞通告。

## 六、参考链接

https://www.cnvd.org.cn/flaw/show/CNVD-2023-08743

## 七、了解更多

深信服千里目安全技术中心持续紧跟国内外漏洞威胁情报，从中筛选出能给客户带来威胁的漏洞，第一时间推送解决方案，持续提供可感知的安全感。在这场永不停歇的攻防战争中，深信服千里目安全技术中心掌握一手漏洞情报，坚持“千里之外，洞悉风险”，与各大网络安全厂商一同维护网络安全，构建平衡、和谐的网络生态系统。关注深信服千里目安全技术中心微信公众号，第一时间了解更多漏洞情报。