网络安全预警通报

2026 年第 8 期（总第 66 期）

西安交通大学网络信息中心 2026 年 08 月 11 日

【预警类型】严重预警

【预警内容】

“Sorry”勒索病毒攻击事件（Linux 服务器安全风险）高危风险漏洞通报

一、漏洞概述

2026 年 8 月 10 日，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室发布安全预警，通报近期我国境内发现多起“Sorry”勒索病毒攻击事件。该病毒属于 2026 年新出现的 Linux 勒索病毒家族，主要针对暴露在互联网中的 Linux Web 服务器开展攻击。

攻击者通常通过互联网暴露的服务器管理系统漏洞、弱口令等方式获取服务器控制权限，随后部署“Sorry”勒索病毒程序，对服务器上的业务文件进行加密，被加密文件会追加.sorry 后缀。在当前情况下，如无有效解密密钥，受害单位通常无法直接恢复被加密数据。

该漏洞具备以下特点：

（1）攻击目标以 Linux Web 服务器为主，互联网暴露资产风险较高；

（2）攻击链涉及服务器管理平台漏洞利用，攻击者可绕过身份认证获取管理权限；

（3）攻击成功后可能导致数据加密、业务中断及敏感信息泄露；

（4）攻击者可能进一步利用弱口令、共享凭证开展横向扩散。

二、漏洞详情

1.技术原理

“Sorry”勒索病毒攻击过程中，攻击者主要针对互联网暴露的 Linux 服务器进行攻击。

攻击流程如下：

第一阶段，攻击者通过扫描互联网资产，发现存在漏洞或弱口令的服务器管理入口。

第二阶段，攻击者利用 cPanel、WHM 以及 WP Squared 等服务器管理系统存在的认证绕过漏洞（CVE-2026-41940）获取未授权访问权限。该漏洞影响 cPanel & WHM 登录认证流程，攻击者无需有效账号即可绕过认证进入管理控制台。

第三阶段，攻击者获得服务器管理权限后，可进一步执行恶意命令，上传并运行勒索病毒程序。

第四阶段，“Sorry”勒索病毒在服务器运行后，会收集系统环境信息，并尝试关闭数据库、安全软件以及备份相关服务，降低安全防护能力。

第五阶段，病毒对服务器文件进行加密处理，并在文件名称后增加.sorry 扩展名，同时留下勒索信息，要求受害单位支付赎金。

2.涉及漏洞详情

漏洞编号　CVE-2026-41940

漏洞名称　cPanel & WHM / WP Squared 认证绕过漏洞

漏洞类型　身份认证绕过

漏洞等级　严重

CVSS 评分　9.8

影响组件　cPanel & WHM、WP Squared

利用方式　远程利用

利用复杂度　低

该漏洞由于服务器管理平台认证机制存在缺陷，攻击者可通过构造特殊请求绕过身份认证，获得管理控制权限。官方已发布安全更新修复该问题。

三、漏洞影响范围

目前确认风险主要涉及：

- 使用 cPanel、WHM、WP Squared 等服务器管理平台的 Linux 服务器；
- 直接暴露互联网的 Linux Web 服务器；
- 未及时安装安全更新的服务器管理系统；
- 使用弱口令或共享密码的服务器环境。

2.威胁严重性

攻击成功后，可能造成以下安全影响：

（1）业务系统不可用

勒索病毒加密网站文件、数据库文件及业务数据，可能导致门户网站、业务系统、中间件服务无法正常运行。

（2）敏感数据泄露

攻击者进入服务器后，可能窃取网站源码、数据库文件、配置文件、用户数据等敏感信息，即使通过备份恢复业务，仍可能存在数据泄露风险。

（3）服务器控制权限丢失

攻击者获取服务器管理员权限后，可创建隐藏账号、植入后门程序，并长期控制服务器。

（4）攻击范围扩大

如果服务器之间存在账号密码复用、共享管理权限等问题，攻击者可能进一步利用 SSH、数据库账号等方式攻击内部其他服务器。

四、处置建议

1.官方修复方案

及时安装安全更新，对于使用 cPanel、WHM、WP Squared 的服务器，应立即升级至官方修复版本。

官方已针对受影响版本发布补丁，建议管理员按照官方指导完成升级。