0x01 漏洞概述

近日，奇安信天眼与安服团队通过数据监控发现，野外出现致远互联旗下致远 A8+协同管理软件，存在远程 Getshell 漏洞。致远互联是中国协同管理软件及云服务领导供应商，专注专注在协同管理软件领域。致远 A8+协同管理软件在很多央企、大型公司都有应用。

致远 A8+在某些版本上存在远程 Getshell 漏洞。**系统某处在无需登录情况下可直接上传任意文件，攻击者一旦上传精心构造的后门文件即可 Getshell，获得目标服务器的权限。目前利用代码已在野外公开，官方提供的补丁程序仍然可利用。**

危害级别：【危急】

验证版本：

A8+V7.0 SP3、A8+ V6.1 SP2

（V6.1 SP1 验证尚不存在，其他版本未验证）

触发条件：没有限制。

0x02 检测方案

奇安信天眼新一代威胁感知系统之前的攻击检测已经可以检测，规则名称为：Java 框架通用代码执行攻击【规则编号 0x10020537】。升级至最新版本 3.

0.0626.11178 或以上版本，会有精准规则检测：致远 A8 系统无需认证 Getshell【0x100206BF】。

同时，可以在天眼新一代威胁感知系统的日志检索中查找” /seeyon/htmlofficeservlet”进行排查。如果发现 POST 提交的恶意数据，并且响应为 200 的数据着重关注。另外，一旦发现上传成功，后门访问路径形如：hxxp://xxx/seeyon/test123456.jsp，请在 seeyon 目录下排查是否有成功上传的后门文件。

0x03 修复建议：

1、 临时缓解措施

- **配置 URL 访问控制策略**

部署于公网的 致远 A8+服务器，可通过 ACL 禁止外网对“/seeyon/htmlofficeservlet”路径的访问。

2、官方补丁

请尽快联系致远官方，索要官方补丁程序。

厂商官网：http://www.seeyon.com/info/company.html