广东省网络与信息安全情况通报

第 59 期

广东省网络与信息安全通报中心　　2019 年 6 月 30 日

关于致远 OA 系统存在任意文件写入高风险隐患的预警通报

工作发现，北京致远互联公司开发的致远 OA 系统存在只能任意文件写入高风险隐患。有关情况预警通报如下:

一、基本情况

6 月 26 日，致远互联公司旗下的致远 A8+协同管理软件某些版本存在任意文件写入漏洞。攻击者在无需登录的情况下，可通过向 URL 为/seeyon/htmlofficeservlet POST 精心构造的数据，即可向目标服务器写入任意文件，写入成功后可执行任意系统命令控制目标服务器。目前已发现有黑客组织掌握该漏洞的利用方式，但官方暂未发布安全补丁。致远互联是中国协同管理软件及云服务领导供应商，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。

二、影响版本

致远 A8-V5 协同管理软件 V6.1sp1

致远 A8+协同管理软件 V7.0、V7.0sp1、V7.0sp2、V7.0sp3

致远 A8+协同管理软件 V7.1

三、临时建议

1、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、配置防火墙过滤规则。

3、修改 Seeyon/A8/ApacheJetspeed/webapps/seeyon/WEB-INF/web.xml 文件。

3、关注官方安全补丁，厂商官网： http://www.seeyon.com/info/company.html。

送：省直和中央驻粤有关单位。

发：各地级以上市公安局网警支队。

（共印 350 份）

审批：石磊　　校稿：金楠　　编校：扈潇潇