关于泛微 OA 产品相关安全措施的说明

近日,监管部门发布了《关于严密防范协同办公等系统遭 受境外黑客组织页面篡改攻击的预警通报》的自查要求,为 配合自查工作,特针对泛微 OA 产品的相关自查给出自查技 术方法以及相关的安全加固建议。

一、自查方法

1、互联网端口开放情况核查

关闭不必要的端口外网映射,如果开放 OA 外网,必须开放的端口有以下,其余端口(如消息服务管理后台(9090)、运维平台(9081)、微搜(8099、8090等))均不需要开放互联网访问(尤其是远程桌面端口(默认 3389 或者 22),务 必不能开放互联网):

ecology: 默认 80 端口

EM6: 默认 89 端口

EM7: 默认 8999 端口

emessage: 默认 7070 和 5222 端口

云桥: 默认 8088 端口;

2、安全补丁检查

▶ Ecology 产品

使用管理员账号登录,访问/wui/secCheck.jsp,进行安全巡检,确保各检测项保持通过状态。

安全补丁地址:

https://www.weaver.com.cn/cs/securityDownload.htm

<u>1</u>#

← → C O 不安全 https://src.e-colog	y.com.cn/wul/secCheck.jsp	☆ 🕹 🛎 :
检查项	检查结果	详情及处置意见
安全包版本检测	检查通过	第600条本次 E9 当時計工包括本: v10.70 量新官時計工包括本: v10.70 当時完全計, 万法已是最新 当時契約律策本: v10.10 量新官時規則考載本: v10.10 当時契約律策本: 24.01.20 量新版本 首何交全計, TEI地E: http://www.weaver.com.cn/cs/securityDownload.html 若存在: 当前交合计TEID已最新成本 若存在: 当前交合计TEID已最新成本
安全包生效性检测	检查通过	已开启安全包防护
JDK版本检测	检查通过	当前JDK版本为: 1.8.0_151 当前JDK版本为可靠版本
检查是否包含webshell后门文件	检查通过	未发现可疑项
sysadmin账号IP白名单限制检测(强烈推荐 启用)	检查通过	整然電気技能以下方常長用PI合体希能(wipa系KD製電位置帯お安全操患,配置后,只有白名单中的PI応者中段能感走常使用 yspadmin使,量化時代用各体希能(wipa系KD製電位置) 修式(xelogy/WEI-INF/securityXML/weaver security custom_rules_1xml,在下方添加如下代码(如果要依行某个网段,影響同P) 的時半段期可,到192.168.7、影响表刊92.168.7、前可以访问): <sysadmin-allow-login-ips> <ip><ip></ip></ip></sysadmin-allow-login-ips>
外网网络新能给我(如果C无五联网动向, 可以包裹和动物资料)	当前0.456450次1993合一端PH12b达2:127.0.0.1、是一个内利。前期43.587.8427 均当前952余容合。端内120年425.557%2914742。要查查到951年一支、那么表示5869 201 201 201 201 201 201 201 201	直看自己当期IP地址的方法: 1. PAPI回答着,可以打开命令提示符题口,windows环境执行ipconfig命令,可以看到自己的机漏IP,可能会有多个IP,比如wifi和有 按注意之个理。 2. 如果想要看自己电脑当前的互联网出口IP,可以后击击毫主儿互联网IP地址。 如果想要不通过,我们认下了要能给: 和外球也让是不,可以近点,看下来到的IP地址是什么。需要联系网络管理员把客户真实IP地址放到X-Forwarded-For头都传给OA成 用,确保oa应用能够拿到真实IP地址。就是上面的页面必须获取到真实客户误P地址
检测器密码	检查通过	无弱密码信息
synccache.jsp 是否是安全版本	检查通过	为安全的synccache.jsp版本
检测bsh补丁是否已经升级	检查通过	bsh补丁已经升级
检测sql注入补丁是否已经升级	检查通过	sqli主入已经升级
检测反序列化补丁是否已经升级	检查通过	反序列化补丁已经升级

▶ EMobile7 产品

访问 EM7 管理后台,检查系统版本,确保系统版本是 20240822 及以上版本

系统补丁地址:

<u>https://emobile.weaver.com.cn/emp/download/downlo</u> <u>ad.html?v=20240229</u>

→ C (8 不安)	https://src.e-cology.com.cn:8443/#/	
		路动管理平台 路动管理平台
		8 用户名
		0.199777
		C 2019
		验证码 1701
		登录
		当前版本:20240822sp2

▶ 云桥产品

访问 http://云桥地址/main/verinfo, 确保系统版本版本是 20231116 及以上版本,且安全补丁版本是 20240725 及以上版本。

 \leftrightarrow \rightarrow C \sim wx.weaver.com.cn/main/verinfo

云桥系统版本: 20240725 安全补丁版本: 20240725

系统补丁地址: <u>https://wx.weaver.com.cn/download/</u> 补丁地址: <u>https://wx.weaver.com.cn/download/security</u>

▶ EMobile6 产品

访问 http://em6 地址/manager, 确保系统版本是 20230530版本,如果低于该版本或者不显示版本号,建议联 系客服或者项目申请 20230530 补丁(025 最新补丁包)升级。

安全补丁版本:应确保安全补丁包版本>=1.7版本。可检查服务器上可以检查 EMobile\webapps\ROOT\WEB-INF\securityUpdateInfo.xml 文件,如果里面的<softeware-version>节点的值为v1.7版本。如低于1.7,可先从以下地址下载补丁升级:

https://www.weaver.com.cn/cs/mobileDownload.html

3、弱口令检查

对于 ecology 产品,可以用管理员登录,访问 /wui/weak.jsp 做基础弱口令排查,确保不存在最明显的弱 口令问题。

对于其他产品,请确保管理员密码不是默认密码或者弱口令。

注: 口令强度建议长度大于 12 位,包含大小字母+特殊字符+数字, 键盘上无明显按键规律:比如 1qaz@WSX3edc 虽然满足复杂度要求,但因为存在明显键盘规律,依然属于弱口令范畴。

二、安全加固措施

1、网络层面

如果有条件,建议接入零信任或者 vpn 进行网络身份认证 防护,将业务系统进行暴露面收敛。

2、ecology 产品

- 登录安全:建议启用双因子登录认证,开启短信动态密码 策略,防范因账号密码泄露导致的安全风险。开启方式如 下:(需要短信设备支持)
 - ✓ 用管理员登录系统,进入后台管理中心->组织权限中 心->账户中心->安全设置->高级设置->动态密码保护, 启用该项设置。

e-cology 后	網擊应用中心	く 🦻 組织权限中心	🤹 流程引擎	🔚 门户引擎	📄 内容引擎	📔 公文管理	1 应用中心	📦 建模引擎	🔆 集成中心	分 升级中心	目 日志中心	🖹 系統 〉	
基础设置	自定义设置	组织结构 账户中心	权限管理 矩阵	信理									
安全设置		🔒 安全设置											
隐私设置		基本设置 高级设置	网段策略	数据库加密									
其他设置		动态密码保护											
			允许作	为登录辅助校验:			-						
			默认启	用方式:			启用		~ 同步	0			
			动态密	码长度:			6						
			动态密	码内容:			数字和字母						-
			有效期	(他):			120						
			登录时	需要登录密码:			-						
			允许作	为二次身份校验:									

 ✓ 点击 组织权限中心→组织结构→批量维护→批量调 整人员信息→系统信息, 左侧选中所有分部, 辅助 校验方式选择动态密码,状态选择启用。

e-cology 后識引擎	版用中心	< () wararto	🔹 流程引牌	🔚 Desiş	🖹 ମନ୍ତ୍ରାଙ୍କ	🖹 公文管理	10 应用中心	🗳 क्षेत्रवाङ्ग	🐥 蛎成中心	🔿 ብቁቀስ	☐ 日志中心	🖹 5.60 >	
2002 0 A		(B89440)	账户中心	权限管理 发	奸管理									
组织维护				比量调整人员信息										保存选中联(2) 🗮
1273 ASI		组织结构			 菜本信 	e ärge	上下级关系	系统信息						
群组设置		* 20	E9TEST		A	國								
99828	*		ର Default ର testsubcompan	y1				🗌 安全级别:		1			<u>^</u>	
NUE 489*	_							SALATION	rst:	动态密码			~	
								☑ 秋志:		启用			~	
					4									

✔ 对于系统管理员账号,需要单独开启,具体步骤如下

e-cology 胞調用户中心	♠ Ⅲ 我的人事 🔛		197	٩						0	• •	* *	h	a ø	٥	• •	• (BASEA .
Ŧ	▲ 系统管理员																	2 2 10 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
9, <u>ज</u> स्र																		1
月 新融人员	金郎 今天 本間 :	本月 本事 本	年															7 花级激素
团 我的非片	(() 法程度并			人力资源 0	Ω	客户进护 0		项目维护 0	(3)	÷	0	财务维护 0	1	物作達 0	ŕ		其他设置 0	
头 我的下属									-									
🗋 BERSERNI	系统操作日志			🙆 安全设)置			/		<								
	EM		展作类型				1					標块			1	/*%地址		
Smith	2024-10-31 09:12:35		102世	54	即校验方式:		动态密码	Ÿ				工作流程			19	2.168.42.93		
A. 2594	2024-10-31 09:22:09		1810	状	志:		息用	*				集成中心			19	2.168.30.14	i .	
	2024-10-31 09:43:46		1000	¢1	定手机号:		13800138000					人力资源			19	2.168.41.6		
◎ 在线人员	2024-10-31 09:43:46		更新	=	次验证密码:		800	¢⊅ 用				人力资源			19	2.168.41.6		
- 	2024-10-31 09:43:59		更新									人力资源			19	2.168.41.6		
尚 人员生日	2024-10-31 10:45:31		更新									人力资源			19	2.168.41.30		
0 48490mm.	2024-10-31 10:52:24		1820							-a22b-		知识管理			10	0.12.102.121		
	2024-10-31 11:53:35		更新						保存			人力资源				2.16.118.8		
	2024-10-31 11:53:35		更新	_	323	世時至人民信息		1期時3				人力资源			15	2.16.118.8		
	2024-10-31 11:53:35		更新		sti	動调整人员信息	t.	」图件4				人力资源			15	2.16.118.8		

注:也可以采用其他的双因子认证方式,比如动态令牌,人脸识别等机制。需要采购对应的产品或者服务支持。

3、EMobile7 产品

建议限制管理账号的 IP 白名单, 配置方式如下:

用 sysadmin 登录 EMobile 后台管理系统->系统管理->安 全设置,按照以下步骤开启 IP 白名单策略及其他相关安全 策略:

法 泛微移动端测试	Ē
命 我的首页	日 安全设置
[] EMobile管理 ~	管理后台登录设置
◇ 云桥第三方APP集成 ~	5
o ^g ECOLOGY集成 →	是否启用登录验证码:
留 应用中心 ~	登录操作最大尝试次数: 10 最大不經过10次
豆 门户管理 マ	管理后台密码策略
□ 消息中心 ~	
■ 统计分析 ~	霉小密码长度: 10 星少为0位,0表示不限制长度,最大不超过10位
A 企业管理 ~	是否必须数字文母大小写及特殊学符:
◎ 系統管理 ▲	管理后公访问限制
缓存信息	
授权信息	是否启用管理后台访问限制: 🚺 设置管理后台只能用指定的IP进行访问
基础设置	TT:+/mtexi08iim=- 172.16.118.8
安全设置	此处填写允许登录管理员账号的终端IP
语言设置	
層性沿澤	タイロを開催した時、支付適能になり、切知: トムンAFLよび日本です。
Mali Contra	登录页备案信息设置

- 三、ecology 安全监控
- ▶异常监控:用 sysadmin 登录,访问 /security/monitor/Monitor.jsp,点击【安全监控】, 查看是否有大量的攻击记录,如果有,可以根据IP封禁 IP
- ▶ 异常文件监控:用 sysadmin 登录,访问 /wui/checkFile.jsp,可以扫描可能存在的后门文件,如 果发现可疑文件,需要人工判断是否是后门,确认是后门, 需要立刻处置,隔离服务器,防止横向扩散攻击。
- ▶ 内存马监控:用 sysadmin 登录,访问 /security/checkHorse.jsp,可以扫描可能存在的内存码, 如果发现可疑内存码,需要人工判断是否是后门,确认是

后门,需要立刻处置,隔离服务器,防止横向扩散攻击。

- ▶ 指定时间内新增或者修改的文件监控:用 sysadmin 登录, 访问/wui/newFile.jsp?dt=2023-07-28, 会扫描出自 2023-7-28日以来系统有过修改的文件。如果发现.jsp文件,需人工判断是否是后门文件,确认是后门,需要立刻 处置,隔离服务器,防止横向扩散攻击。
- ▶ 用户登录日志监控:登录管理员,后台管理中心->日志中 心->登录失败日志,检查是否存在频繁爆破日志以及是 否存在可疑登录
- ➤系统安全日志监控:用 sysadmin 登录,访问 /security/monitor/Monitor.jsp,点击【日志安全详情】, 查看是否有大量的攻击记录,如果有,可以根据 IP 封禁 IP (重点关注外网 IP 的攻击情况)
- ➤ Webshell 扫描: 使用 D 盾扫描项目路径下是否存在可疑 webshell 文件

D 盾下载地址及使用说明: <u>https://www.d99net.net/</u>

注:如果扫描结果中出现级别为5的,那么基本确定是后 门文件。 该软件仅适用 windows, linux 无法使用。如果要扫描, 需要把应用目录打包到 windows 环境扫描。

泛微网络科技股份有限公司

2024-10-31