天际友盟
TianJi Partners

强化防线：防守方的重大演练安全防护手册

2023.8

双子座实验室

1. 概述

大型攻防演练从 2016 年开始，今年已经是第 7 个年头。攻防演练是指在真实网络环境下以获取指定目标系统的管理权限为目地的攻击，通过攻防演练，旨在全面评估防守方所在网络的整体安全防护能力及应急响应能力。

伴随着 2023 年攻防演练大幕的拉开，攻击方目前可谓摩拳擦掌，准备在这场挑战中大展身手。然而在复杂的网络环境下，相较于攻方没有后顾之忧，可以灵活实施多种战术的情况，防守方虽蓄势以待，却因拥有的庞大资产体系和架构，可能随时面临着防守阵地被突破的处境。天际友盟双子座实验室根据近年的实际演练情况，从防守方的角度切入，提供了一份可参考的网络安全防护策略，主要包括设备和漏洞篇两大部分。本文将首先分析防守方设备的潜在攻击面和可能面临的攻击手段；其次，结合最近几个月国内外热门设备和软件的漏洞情况，提供详细的漏洞参考列表，以帮助蓝方识别和应对关键漏洞，降低红方利用 0day 或 1day 等漏洞进行攻击的风险，希望下面的内容能对防守方有所帮助。

2. 设备篇

攻守对抗下，对于防守方而言，选择将视线聚焦在易受攻击的目标设备之上，针对性地加强高风险设备的保护措施至关重要。以下我们将从电脑端、移动端、网络设备、工控设备分别列举常见的易受攻击设备及软件的类型、攻击手段、并为用户提供相应的防范建议。

2.1电脑端

2.1.1 易受攻击的电脑端设备

◆ 操作系统

操作系统是计算机设备的核心软件，由于其复杂性，难免存在漏洞，加上其安全性往往依赖于用户的行为，在全球范围内均存在被攻击的风险。一旦渗透，攻击者便可以获取对目标设备的完全控制权。目前，已知的常被攻击的系统包括：Windows XP、Windows 7、Windows 8/8.1、Windows Server 2003、Windows 10、macOS 以及 Linux 系统发行版的旧版本。

◆ Web 浏览器

Web 浏览器作为主要的上网工具，用户众多，也因软件漏洞、插件和扩展程序等安全性问题而使得攻击变得更加容易。成功入侵后，攻击者可以窃取用户的敏感信息（如账号密码、信用卡信息）或进行恶意操作，例如篡改网页内容、植入恶意代码等。目前，已知的常被攻击的浏览器包括：旧版本的 IE，存在漏洞的 Chrome、Firefox、Safari 等。

◆ 第三方应用程序

第三方应用程序通常由不同的开发人员进行开发和维护，并且需要与其他设备和服务进行交互，因此极有可能存在漏洞和不安全的权限管理。攻击者可以通过漏洞利用、供应链攻击等手段，使整个第三方软件的供应链环节受到严重影响，可能导致大规模数据泄露等严重后果。目前，已知的常被攻击者利用的软件包括：Adobe Flash Player、Java Runtime Environment、Microsoft Office、企业级 OA 办公系统、浏览器扩展程序、媒体解码器和播放器、安全工具、社交媒体程序、VPN 软件、翻译软件、银行支付应用、PDF 阅读器等。

◆ **数据库**

数据库在各种应用程序和系统中被广泛使用，主要用于存储大量敏感数据。但由于数据库本身存在漏洞利用(如 SQL 注入)的机会，数据库管理员(DBA)又通常拥有高级权限，因此通过攻击数据库，攻击者更容易从内部获取更多权限、进而实施数据泄露、数据篡改、勒索加密等恶意攻击。目前，已知的常被攻击的数据库包括：MySQL、Microsoft SQL Server、广泛应用于商业环境中的 Oracle Database、默认配置不安全的 MongoDB、默认情况下没有进行身份验证和访问控制的 Redis 等。

2.1.2 攻击手段

攻击者常用的针对电脑端设备的攻击手段

- 漏洞利用、钓鱼攻击、社会工程学、供应链攻击、DDoS 攻击、勒索软件、病毒木马等。

2.1.3 防范建议

1) 提高安全意识，及时更新计算机操作系统和升级系统内的各种软件，及时修复组件漏洞；

2) 谨防钓鱼攻击，使用可信任的软件源和供应商；

3) 强化访问控制，使用强密码和多因素身份验证；

4) 定期备份和加密重要数据，定期进行安全评估和漏洞扫描；

5) 配置防火墙和安全软件，使用网络安全设备或组件阻断相关指示器。

2.2移动端

2.2.1 易受攻击的移动端设备

◆ 智能手机操作系统

智能手机操作系统内部信息价值大，复杂性高，可能存在未知的安全漏洞，但供应商却无法及时更新和修复已知漏洞，这使得此类设备更容易遭受攻击。一旦攻陷，攻击者就可以造成隐私泄露、经济损失等严重影响。目前，已知的常被攻击的智能手机操作系统包括：应用广泛的 Android 系统、存在漏洞的 iOS 系统、基于 Android 的国产自定义系统(如华为的 EMUI、小米的 MIUI)等。

◆ 应用程序商店

应用程序商店是用户获取应用程序的主要渠道，常被攻击者利用其审核和筛选不严格的特点进行中间人和钓鱼欺诈攻击。成功突破，攻击者就能够通过诱导用户下载和使用恶意软件或篡改后的正常应用程序，致使信息泄露、设备受损等问题。目前，已知的常被攻击者部署恶意软件的应用程序商店包括：官方应用商店(如 Google Play、App Store、应用宝、360 手机助手、小米应用商店、华为应用市场等)、应用商店的克隆版本、第三方应用平台等。

◆ 社交媒体程序

社交媒体应用程序是最常用的沟通工具之一，同时也是攻击者进行钓鱼和社工的重点目标。原因是用户通常未能谨慎对待未知来源的消息，因此攻击者可以通过伪造短信或社交媒体应用的通知传播恶意软件、窃取用户的敏感信息，进而用于身份诈骗、盗取资金或其它非法活动。目前，已知的常被攻击者利用的社交媒体程序包括：短信、微信、微博、抖音、QQ、LinkedIn、WhatsApp、Telegram 等。

2.2.2 攻击手段

攻击者常用的针对移动端设备的攻击手段

- 钓鱼欺诈、社会工程学、漏洞利用、病毒木马、勒索软件等。

2.2.3 防范建议

1) 提高安全意识，及时更新智能手机操作系统和升级应用软件；

2) 安装可靠的安全软件和防病毒工具；

3) 谨防钓鱼攻击，谨慎点击来源不明短信链接和社交媒体消息；

4) 定期备份和加密重要数据。

2.3 网络设备

2.3.1 易受攻击的网络设备

◆ 路由器

路由器作为连接家庭或办公室网络与互联网之间的关键设备，通常由于存在的各种漏洞和安全弱点而得到攻击者青睐。一旦攻陷，攻击者就可以完全控制网络流量，通过构建僵尸网络，进行大规模网络攻击，最终导致服务不可用、数据泄露和网络瘫痪等严重后果。目前，已知的常被攻击的路由器品牌包括：华为、小米、华硕、MikroTik、TP-LINK、Cisco、GPON、D-Link、Realtek 等。

◆ 交换机

交换机是用于在局域网内进行数据包转发的设备，也往往由于各种漏洞以及不安全的配置和访问控制而成为重点攻击对象。通过渗透交换机，攻击者可以监视、篡改或拦

截经过交换机的数据流量，获取敏感信息并影响网络通信，甚至可能导致网络瘫痪或被用于进一步的恶意活动。目前，已知的常被攻击的交换机品牌包括：华为、中兴、海康威视、Cisco、HPE/Aruba、Juniper、D-Link 等。

◆ **防火墙**

防火墙主要负责监控和过滤网络流量，其安全性高度依赖于正确的配置，倘若配置不当或存在漏洞，也极易遭受攻击。成功入侵，攻击者可以绕过防护机制，直接访问内部网络，导致敏感数据泄露、系统瘫痪以及其他安全风险。目前，已知的常被攻击的防火墙品牌包括：商业防火墙(如华为、深信服、Cisco 、Fortinet 、Palo Alto Networks)、开源防火墙(如 pfSense、IPFire、OPNsense)、UTM 设备、云防火墙(如腾讯云、阿里云、华为云、百度云、AWS 、Azure)等。

2.3.2 攻击手段

攻击者常用的针对网络端设备的攻击手段

- 漏洞利用、僵尸网络、拒绝服务攻击、ARP 欺骗攻击、中间人攻击等。

2.3.3 防范建议

1) 提高安全意识，及时更新固件和软件，修复组件漏洞；

2) 强化访问控制，使用强密码和多因素身份验证，仅允许受信任的 IP 地址或网络进行管理访问；

3) 配置适当的防火墙规则、访问控制列表（ACL）和安全策略，仅开放必需的网络服务和端口；

4) 部署入侵检测和防御系统（IDS/IPS），定期备份设备配置和日志文件，使用网络安全设备或组件阻断相关指示器；

5) 使用安全的协议（如 HTTPS）进行加密通信或建立 VPN 隧道。

2.4 工控设备

2.4.1 易受攻击的工控设备

◆ 工业自动化系统

工业自动化系统可对生产线中的各个环节进行自动化控制和管理，因此往往需要与企业内部网络或互联网进行连接，但由于此类设备通常未及时修补安全漏洞以及缺乏充分的网络安全措施，攻击者十分可能利用漏洞以及网络通道突破防线，获取对系统的控制权，进而操纵生产过程、篡改数据和程序，最终导致生产中断、产品质量下降甚至造成设备损坏或人员伤亡等严重后果。目前，已知的常被攻击的工业自动化系统品牌包括：西门子、施耐德电气、ABB、倍福、欧姆龙、GE、罗克韦尔等。

◆ 工业机器人

工业机器人广泛应用于制造业，由于机器人系统的特殊性质和复杂性，供应商通常未能及时提供安全更新和补丁，这使得机器人系统更容易受到已知漏洞的攻击。同样，工业机器人通常需要与其他设备、互联网或内部网络相连，攻击者可以通过这些渠道获得对机器人的远程控制权，进而篡改程序并造成生产过程中的故障。目前已知的常用的被攻击的工业机器人品牌包括：ABB、Fanuc、KUKA、Yaskawa 等。

2.4.2 攻击手段

攻击者常用的针对工控设备的攻击手段

- 漏洞利用、无线攻击、恶意软件、物理攻击、DDoS 攻击、供应链攻击

2.4.3 防范建议

1) 提高安全意识，及时更新系统软件，及时修复组件漏洞；

2) 强化访问控制，定期审查和维护用户账户和权限列表，使用强密码和多因素身份验证，限制对工业自动化系统和机器人的物理和远程访问权限；

3) 实施网络隔离，将工业自动化系统和机器人与其他网络分开；

4) 定期进行安全测试和漏洞扫描，定期进行数据备份。

结合易受攻击的设备的特点，我们给出了针对性的防范建议。那么在实际网络环境中，哪些设备存在严重的漏洞呢？它们的影响范围又如何呢？接下来我们介绍下一章——漏洞篇。

3. 漏洞篇

上一章节我们介绍了易受攻击的设备，在了解了这些设备存在的弱点以及攻击者可利用的手段之后，我们将重点披露国内外设备及软件的热门漏洞，基于漏洞名称、危险等级、漏洞编号、影响版本等方面对漏洞详情进行描述，并结合前一章设备篇，对各个漏洞所属设备/应用类别进行归类，同时为漏洞防护给出安全建议或修补策略。

3.1 国内产品热点漏洞披露

（1）达梦企业管理器（DEM）存在未授权访问漏洞，攻击者可以利用该漏洞未授权访问存在重要数据的接口。

漏洞名称	达梦企业管理器存在未授权访问漏洞	危险等级	中危
漏洞编号	CNVD-2023-52177	影响版本	3.3.6
有无公开 POC/EXP	无		
针对设备	Web 管理器		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁：https://www.dameng.com/list_103.html			

（2）杭州海康威视数字技术股份有限公司 iVMS-8700 综合安防管理平台存在文件上传漏洞，攻击者可利用该漏洞上传恶意文件。

漏洞名称	杭州海康威视数字技术 iVMS-8700 综合安防管理平台文件上传漏洞	危险等级	高危
漏洞编号	CNVD-2023-53133	影响版本	V2.0.0 - V2.9.2

有无公开 POC/EXP	有		
针对设备	第三方应用程序：Web 管理平台		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.hikvision.com			

（3）IBOS OA SQL 注入漏洞：IBOS 是一个协同办公管理系统。IBOS OA 4.5.5 版本存在 SQL 注入漏洞，该漏洞源于组件中的参数 id 缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行 SQL 语句，进行数据窃取等操作。

漏洞名称	IBOS OA SQL 注入漏洞	危险等级	中危
漏洞编号	CVE-2023-3478 CNVD-2023-54865	影响版本	4.5.5
有无公开 POC/EXP	有		
针对设备	第三方应用程序：OA 办公系统		
防御/缓解措施			

目前厂商已发布漏洞修复程序，建议受影响的用户及时联系厂商安装安全补丁：http://www.ibos.com.cn/download

（4）泛微 e-cology SQL 注入漏洞：泛微 e-cology 版本 10.58.0 之前存在 SQL 注入漏洞，攻击者可以通过拼接语句执行 SQL 命令，从而利用该漏洞获取数据库中的敏感信息并进一步执行恶意操作。

漏洞名称	泛微 e-cology SQL 注入漏洞	危险等级	中危
漏洞编号	CVE-2023-3793	影响版本	<10.58.0
有无公开 POC/EXP	有		
针对设备	第三方应用程序：OA 办公系统		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁：https://www.weaver.com.cn/cs/securityDownload.asp#			

（5）用友畅捷通 T+ SQL 注入漏洞：畅捷通 T+存在 SQL 注入漏洞，攻击者可利用此漏洞在未授权的情况下执行任意 SQL 语句，最终造成服务器敏感性信息泄露或远程命令执行。

漏洞名称	畅捷通 T+ SQL 注入漏洞	危险等级	高危
漏洞编号	暂无	影响版本	v13.0 v16.0
有无公开 POC/EXP	有		
针对设备	第三方应用程序：会计财务软件		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.chanjetvip.com/product/goods/			

（6）用友畅捷通 T+远程命令执行漏洞：用友畅捷通 T+存在前台远程代码执行漏洞，攻击者可利用 GetStoreWarehouseByStore 方法注入序列化的载荷，执行任意命令，最终造成服务器信息泄露或者代码执行。

漏洞名称	畅捷通 T+ 远程命令执漏洞	危险等级	高危
漏洞编号	暂无	影响版本	v13.0 v16.0
有无公开 POC/EXP	有		

针对设备	第三方应用程序：会计财务软件
防御/缓解措施	
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.chanjetvip.com/product/goods/detail?id=6077e91b70fa071069139f62	

（7）泛微 E-Cology9 任意用户登录漏洞：由于泛微 E-Cology9 存在一个信息泄露接口，攻击者在未授权的情况下，可利用该接口获取系统已注册的用户，随后攻击者可以利用获取到的用户名构造恶意数据，模拟任意用户登录后台。

漏洞名称	泛微 E-Cology9 任意用户登录漏洞	危险等级	高危
漏洞编号	暂无	影响版本	<10.57.1
有无公开 POC/EXP	有		
针对设备	第三方应用程序：OA 办公系统		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁：			

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

（8）泛微 E-Cology XML 外部实体注入漏洞：攻击者可绕过现有防护实现 XML 外部实体注入攻击，最终可能造成敏感信息泄露，甚至可能配合其他漏洞造成远程命令执行等危害。

漏洞名称	泛微 E-Cology XML 外部实体注入漏洞	危险等级	高危
漏洞编号	暂无	影响版本	泛微 EC 9.x 且补丁版本 < 10.58.2 泛微 EC 8.x 且补丁版本 < 10.58.2
有无公开 POC/EXP	有		
针对设备	第三方应用程序：OA 办公系统		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.weaver.com.cn/cs/securityDownload.html#			

（9）Smartbi 登录代码逻辑漏洞：攻击者可利用此漏洞绕过身份认证，进一步结合后台接口实现远程代码执行。

漏洞名称	Smartbi 登录代码逻辑漏洞	危险等级	高危
漏洞编号	暂无	影响版本	V9
有无公开 POC/EXP	有		
针对设备	第三方应用程序		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁。用户可通过自动更新或者手动更新的方式进行漏洞修复。补丁链接如下： https://www.smartbi.com.cn/patchinfo			

（10）宏景 eHR SQL 注入漏洞：攻击者可利用此漏洞执行任意 SQL 语句，从而窃取数据库敏感信息，甚至执行命令。

漏洞名称	宏景 eHR SQL 注入漏洞	危险等级	高危
漏洞编号	CNVD-2023-08743	影响版本	< 8.2
有无公开 POC/EXP	有		

针对设备	第三方应用程序：人力资源管理系统
防御/缓解措施	
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： http://www.hjsoft.com.cn/	

(11) 北京神州绿盟科技有限公司 NFNX3 存在二进制漏洞：攻击者可利用该漏洞获取服务器权限。

漏洞名称	绿盟科技 NFNX3 存在二进制漏洞	危险等级	高危
漏洞编号	CNVD-2023-39090	影响版本	NFNX3 6.0.Ess 8560P18
有无公开 POC/EXP	无		
针对设备	防火墙		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： http://update.nsfocus.com/update/listNewNfbDetail/v/v7.0			

（12）锐捷 Networks Product 安全漏洞：锐捷 Networks Product 存在安全漏洞，该漏洞源于允许远程攻击者通过对/cgi-bin/luci/的 POST 请求来升级 API 权限。

<table>
<tr><td>漏洞名称</td><td>锐捷 Networks Product 安全漏洞</td><td>危险等级</td><td>高危</td></tr>
<tr><td>漏洞编号</td><td>CVE-2023-34644</td><td rowspan="2">影响版本</td><td rowspan="2">RG-EW series home routers EW_3.0(1)B11P204
RG-NBS and RG-S1930 series switches SWITCH_3.0(1)B11P218
RG-EG series business VPN routers EG_3.0(1)B11P216
EAP
RAP series wireless access points AP_3.0(1)B11P218
NBC series wireless controllers AC_3.0(1)B11P86</td></tr>
<tr><td>有无公开 POC/EXP</td><td>无</td></tr>
<tr><td>针对设备</td><td colspan="3">路由器</td></tr>
<tr><td colspan="4">防御/缓解措施</td></tr>
</table>

目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.ruijie.com.cn/gy/xw-aqtg-gw/91389/

3.2 国外产品热点漏洞披露

（1）Microsoft Excel 代码执行漏洞: Microsoft Excel 存在代码执行漏洞，攻击者可利用该漏洞在系统上执行任意代码。

<table>
<tr><td>漏洞名称</td><td>Microsoft Excel 代码执行漏洞</td><td>危险等级</td><td>高危</td></tr>
<tr><td>漏洞编号</td><td>CVE-2023-33137

CNVD-2023-53909</td><td rowspan="2">影响版本</td><td rowspan="2">Microsoft Excel 2013 SP1

Microsoft Excel 2013 RT SP1

Microsoft Excel 2016

Microsoft Office Online Server

Microsoft Office 2019</td></tr>
<tr><td>有无公开 POC/EXP</td><td>有</td></tr>
<tr><td>针对设备</td><td colspan="3">第三方应用程序：办公软件</td></tr>
<tr><td colspan="4">防御/缓解措施</td></tr>
</table>

目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-33137

（2）WordPress plugin User Registration 代码问题漏洞：WordPress plugin User Registration 3.0.2 版本及之前版本存在漏洞，该漏洞由于采用硬编码加密密钥并且缺少对文件类型的验证，攻击者可利用该漏洞上传任意文件，从而远程执行代码。

漏洞名称	WordPress plugin User Registration 代码问题漏洞	危险等级	高危
漏洞编号	CNNVD-202307-1239	影响版本	<=3.0.2
有无公开 POC/EXP	无		
针对设备	第三方应用程序：CMS 插件		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.wordfence.com/threat-intel/vulnerabilities/id/a979e885-f7dd-4616-a881-64f3d97c309d?source=cve			

（3）Apache Shiro 身份验证绕过漏洞：当漏洞版本 Shiro 与基于非规范化路由的 API 或其他 Web 框架一起使用时，可能导致身份验证绕过。

漏洞名称	Apache Shiro 身份验证绕过漏洞	危险等级	高危
漏洞编号	CVE-2023-34478	影响版本	Apache Shiro 版本 < 1.12.0 Apache Shiro 版本 < 2.0.0-alpha-3
有无公开 POC/EXP	无		
针对设备	第三方应用程序：Web 安全框架		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁：https://github.com/apache/shiro/tags			

（4）OpenSSH ssh-agent 远程代码执行漏洞：攻击者可以利用该漏洞在某些条件下通过转发的代理套接字远程执行代码。

漏洞名称	OpenSSH ssh-agent 远程代码执行漏洞	危险等级	高危
漏洞编号	CVE-2023-38408	影响版本	< 9.3p2

有无公开POC/EXP	有		
针对设备	第三方软件：OpenSSH		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.openssh.com/			

（5）Confluence Data Center & Server 远程代码执行漏洞：经过身份验证的攻击者可利用该漏洞执行任意代码，此外攻击者利用该漏洞不需要用户交互。

漏洞名称	Confluence Data Center & Server 远程代码执行漏洞	危险等级	高危
漏洞编号	CVE-2023-22508	影响版本	7.19.8 <= version<8.2.0
有无公开POC/EXP	无		
针对设备	第三方应用程序：文档协同软件		
防御/缓解措施			

目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.atlassian.com/software/confluence/download-archives

（6）Confluence Data Center & Server 远程代码执行漏洞：经过身份验证的高权限攻击者可利用该漏洞执行任意代码，此外，攻击者利用该漏洞不需要用户交互。

<table>
<tr><td>漏洞名称</td><td>Confluence Data Center & Server 远程代码执行漏洞</td><td>危险等级</td><td>高危</td></tr>
<tr><td>漏洞编号</td><td>CVE-2023-22505</td><td rowspan="2">影响版本</td><td rowspan="2">8.0.0</td></tr>
<tr><td>有无公开 POC/EXP</td><td>无</td></tr>
<tr><td>针对设备</td><td colspan="3">第三方应用程序：文档协同软件</td></tr>
<tr><td colspan="4">防御/缓解措施</td></tr>
<tr><td colspan="4">目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁：
https://www.atlassian.com/software/confluence/download-archives</td></tr>
</table>

（7）Bamboo Data Center & Server 远程代码执行漏洞：经过身份验证的攻击者可利用该漏洞执行任意代码，此外，攻击者利用该漏洞不需要用户交互。

漏洞名称	Bamboo Data Center & Server 远程代码执行漏洞	危险等级	高危
漏洞编号	CVE-2023-22506	影响版本	8.0.0 - 9.2.3 <=9.3.1
有无公开POC/EXP	无		
针对设备	第三方平台		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.atlassian.com/software/confluence/download-archives			

（8）GitLab 访问控制不当漏洞： GitLab 企业版（EE）中的一个访问控制不当漏洞，攻击者可利用该漏洞更改公共顶级组的名称或路径。

漏洞名称	GitLab 访问控制不当漏洞	危险等级	高危
漏洞编号	CVE-2023-3484		12.8<=version<15.11.11

有无公开POC/EXP	无	影响版本	16.0<=version<16.0.7 16.1<=version<16.1.2
针对设备	代码管理平台 GitLab		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://about.gitlab.com/update/			

（9）Apache Shiro 目录穿越漏洞：攻击者可利用该漏洞，构造恶意数据执行目录穿越攻击，最终造成身份认证绕过。

漏洞名称	Apache Shiro目录穿越漏洞	危险等级	高危
漏洞编号	CVE-2023-34478	影响版本	version< 1.12.0 2.0.0 ⩽ version< 2.0.0-alpha-3
有无公开POC/EXP	无		
针对设备	第三方应用程序：Java 安全框架		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁：			

https://about.gitlab.com/update/

（10）Gitlab 任意文件读取漏洞：该漏洞由于未对文件路径进行过滤，攻击者可利用该漏洞，构造恶意数据执行目录遍历攻击，读取任意文件，造成受害服务器信息泄露。

漏洞名称	Gitlab 任意文件读取漏洞	危险等级	高危
漏洞编号	CVE-2023-2825	影响版本	GitLab CE 16.0.0 GitLab EE 16.0.0
有无公开 POC/EXP	有		
针对设备	代码管理平台 GitLab		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁。 https://about.gitlab.com/update/			

（11）Microsoft Office 权限提升/命令执行漏洞：攻击者可以利用此漏洞在 Outlook 应用程序中附加一个恶意的 WORD 文件，当用户打开文件后，文件可执行其携带的恶意命令。

漏洞名称	Microsoft Office 权限提升/命令执行漏洞	危险等级	高危
漏洞编号	CVE-2023-33148	影响版本	18.2305.1222.0
有无公开POC/EXP	有		
针对设备	第三方应用程序：办公软件		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://msrc.microsoft.com/update-guide/releaseNote/2023-Jul			

（12）Openfire 身份认证绕过漏洞: Openfire 的 Web 管理后台存在一处目录穿越漏洞，攻击者可利用该漏洞绕过权限校验，访问所有受限页面。此外，攻击者还可借此漏洞在未授权的情况下创建管理员用户，并结合后台自定义插件的上传，失陷远程命令执行。

漏洞名称	Openfire身份认证绕过漏洞	危险等级	高危
漏洞编号	CVE-2023-32315		3.10.0<= version< 4.6.8

有无公开POC/EXP	有	影响版本	4.7.0 <= version< 4.7.5
针对设备	第三方应用：即时通讯服务		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://github.com/igniterealtime/Openfire/releases			

(13) Apache Tomcat 信息泄露漏洞：如果响应没有设置任何 HTTP 标头，则不会发送 AJP 协议的 SEND_HEADERS 消息，这意味着至少有一个基于 AJP 协议的代理（mod_proxy_AJP）会将前一个请求的响应标头作为当前请求的响应标头，导致信息泄露。

漏洞名称	Apache Tomcat 信息泄露漏洞	危险等级	高危
漏洞编号	CVE-2023-34981	影响版本	11.0.0-M5 10.1.8 9.0.74 8.5.88
有无公开POC/EXP	无		

针对设备	Web 应用服务器
防御/缓解措施	
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://tomcat.apache.org/	

(14) Progress MOVEit Transfer SQL 注入漏洞：MOVEit Transfer Web 应用程序中存在 SQL 注入漏洞，可在未经身份验证的情况下利用该漏洞获得对 MOVEit Transfer 数据库的未授权访问、提升权限或远程执行代码。

漏洞名称	Progress MOVEit Transfer SQL 注入漏洞	危险等级	高危
漏洞编号	CVE-2023-34362 CVE-2023-36934 CVE-2023-36933 CVE-2023-36932	影响版本	低于以下版本： 2021.0.6 (13.0.6), 2021.1.4 (13.1.4), 2022.0.4 (14.0.4), 2022.1.5 (14.1.5) 2023.0.1 (15.0.1)
有无公开 POC/EXP	有		
针对设备	第三方应用程序：数据传输软件		
防御/缓解措施			

目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023

(15) Apache RocketMQ 远程代码执行漏洞:当 RocketMQ 的 NameServer 组件暴露在外网，且缺乏有效的身份认证时，攻击者可以利用更新配置功能，以 RocketMQ 运行的系统用户身份执行任意命令。

漏洞名称	Apache RocketMQ 远程代码执行漏洞	危险等级	高危
漏洞编号	CVE-2023-37582	影响版本	< 4.9.7 < 5.1.2
有无公开 POC/EXP	有		
针对设备	第三方应用程序：中间件		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://rocketmq.apache.org/download/			

(16) Google Chrome V8 类型混淆漏洞：攻击者可通过诱导用户打开恶意链接来利用此漏洞，从而在应用程序上下文中执行任意代码。目前，此漏洞已检测到在野利用。

<table>
<tr><td>漏洞名称</td><td>Google Chrome V8 类型混淆漏洞</td><td>危险等级</td><td>高危</td></tr>
<tr><td>漏洞编号</td><td>CVE-2023-3079</td><td rowspan="2">影响版本</td><td rowspan="2">< 114.0.5735.110
< 114.0.5735.106
< 114.0.5735.106</td></tr>
<tr><td>有无公开 POC/EXP</td><td>无</td></tr>
<tr><td>针对设备</td><td colspan="3">Web 浏览器</td></tr>
<tr><td colspan="4">防御/缓解措施</td></tr>
<tr><td colspan="4">目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁。用户可通过自动更新或者手动更新的方式进行漏洞修复:
https://google.cn/chrome/</td></tr>
</table>

(17) Grafana Azure Active Directory 身份验证绕过漏洞：攻击者可以通过创建一个拥有与用户账户相同的电子邮件地址的恶意帐户，利用该漏洞绕过身份验证，从而接管用户账户。

漏洞名称	Grafana Azure Active Directory 身份验证绕过漏洞	危险等级	高危

漏洞编号	CVE-2023-3128	影响版本	11.0.0-M5 10.1.8 9.0.74 8.5.88
有无公开POC/EXP	有		
针对设备	第三方应用程序：数据可视化平台		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://tomcat.apache.org/			

(18) VMware Aria Operations 命令注入漏洞：攻击者可以通过特制的请求将恶意命令拼接注入，从而远程执行命令。

漏洞名称	VMware Aria Operations 命令注入漏洞	危险等级	高危
漏洞编号	CVE-2023-20887	影响版本	6.2.0<=version <= 6.10.0
有无公开POC/EXP	有		
针对设备	第三方应用程序：虚拟化应用程序		

防御/缓解措施
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://www.vmware.com/security/advisories/VMSA-2023-0012.html

(19) Windows HTTP.sys 权限提升漏洞：由于 HTTP.sys 在拷贝 ServiceName 时存在整数溢出漏洞，攻击者可以构造恶意程序触发该漏洞，成功利用此漏洞可实现权限提升或拒绝服务。

漏洞名称	Windows HTTP.sys 权限提升漏洞	危险等级	高危
漏洞编号	CVE-2023-23410	影响版本	Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
有无公开 POC/EXP	无		

			Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2016 (Server Core installation) Windows Server 2016

			Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems

			Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022

			Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems
针对设备	操作系统：Windows		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁： https://msrc.microsoft.com/update-guide/releaseNote/2023-Mar			

(20) Schneider Electric & APC Easy UPS 代码执行漏洞：Schneider Electric 和 APC Easy UPS Online Monitoring Software 中存在大小写处理不当，当通过 Java RMI 接口操纵内部方法时，可能导致远程代码执行。

漏洞名称	Schneider Electric & APC Easy UPS 代码执行漏洞	危险等级	高危
漏洞编号	CVE-2023-29412	影响版本	APC Easy UPS Online Monitoring Software 版本：<= V2.5-GA-01-22320（Windows 10、11、Windows Server 2016、2019、2022） Schneider Electric Easy UPS Online Monitoring Software 版本：<= V2.5-GS-01-22320（Windows 10、11、Windows Server 2016、2019、2022）
有无公开 POC/EXP	无		
针对设备	工控软件：施耐德电气 UPS 在线监控系统		
防御/缓解措施			
目前厂商已发布漏洞补丁，建议受影响的用户及时联系厂商安装安全补丁：			

APC 下载链接（适用于 Windows 10 版本）：https://download.schneider-electric.com/files?p_enDocType=Software+-+Release&p_Doc_Ref=APC_install_APC_UPS_windows Schneider Electric 下载链接（适用于 Windows 10 版本）：https://download.schneider-electric.com/files?p_enDocType=Software+-+Release&p_Doc_Ref=Install_Schneider_UPS_windows

(21) SIMATIC 多个产品权限提升漏洞：受影响的产品包含一个数据库管理系统，该系统可能允许具有低权限的远程用户使用对服务器有影响的数据库的嵌入式功能（本地或网络共享中）。 对服务器网络具有网络访问权限的攻击者可以利用这些嵌入式功能在数据库管理系统的服务器中以提升的权限运行代码。

漏洞名称	SIMATIC 多个产品权限提升漏洞	危险等级	高危
漏洞编号	CVE-2023-29412	影响版本	SIMATIC PCS 7(ALL VERSION) SIMATIC S7-PM(ALL VERSION) SIMATIC STEP 7 V5(VERSION<5.7)
有无公开 POC/EXP	无		

针对设备	工控软件：SIMATIC 控制器
防御/缓解措施	
目前厂商已发布漏洞缓解措施，用户可访问下方链接查看缓解措施： https://cert-portal.siemens.com/productcert/html/ssa-968170.html	

3.3 针对漏洞的防范措施

3.3.1 具体应对措施

1) 确认组织的资产情况，对所有服务器和暴露在外的服务进行全方位扫描，根据漏扫结果依次按优先级从高到低逐个打补丁，如果遇到不能升级的设备或升级影响业务运行的服务，则必须寻找可靠的替换方法，同时重点关注这些服务器的运行状态和异常告警；

2) 参考近期披露的国内外高危漏洞列表，查看本组织内部是否使用相应设备或服务，及时采取措施进行修护；

3) 定期扫描服务器，更新系统补丁，对零日或最新披露的漏洞及时进行防护；

4) 制定详细的应急响应计划，一旦发现通过漏洞入侵的攻击，立即采取有效措施进行阻断或隔离。

3.3..2 其他必要防范措施

1) 所有服务器、终端应强行实施复杂密码策略，杜绝弱密码，杜绝使用通用密码管理所有机器；

2) 安装杀毒软件、终端安全管理软件，并及时更新病毒库；

3) 服务器开启关键日志收集功能，为安全事件的追踪溯源提供支撑；

4) 加强系统和网络的访问控制，修改防火墙策略，关闭非必要的应用端口或服务，减少将危险服务（如 SSH、RDP 等）暴露到公网的可能性，减少攻击面；

5) 使用企业级安全产品，提升企业的网络安全性能，同时还可结合威胁情报中的漏洞情报提升对高危漏洞和零日漏洞的响应与发现能力，做到及时预判漏洞影响，迅速落实漏洞的防范或缓解措施。

4. 总结

综上所述，为了能够在攻防演练这场网络对抗中取得胜利，建议防守方将以上内容作为核查自身安全体系和安全产品特性的参考手册，以加强对系统薄弱环节的认知，并尽可能降低人为因素的影响。不过，仅凭以上内容当然不够，最重要的还是要做到快速高效的应急响应，及时获取有针对性的威胁情报，以在真正的攻击演练中实现对相关 IOCS 的快速封禁或阻断。

欢迎联系我们

联系邮箱：mkt@tj-un.com

电话：400-0810-700