安全漏洞通告

CVE-2021-35464: ForgeRock AM 远程代码执行漏洞通告

360CERT
北京奇虎科技有限公司

报告信息

报告名称	CVE-2021-35464: ForgeRock AM 远程代码执行漏洞通告		
报告类型	安全漏洞通告	报告编号	B6-2021-063002
报告版本	1	报告日期	2021-06-30
报告作者	360CERT	联系方式	g-cert-report@360.cn
提供方	北京鸿腾智能科技有限公司-360CERT		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2021-06-30	360CERT	360CERT	撰写报告

目录

1 漏洞简述

2021 年 06 月 30 日，360CERT 监测发现 portswigger 发布了 ForgeRockAM远程代码执行漏洞 的漏洞分析报告，漏洞编号为 CVE-2021-35464 ，漏洞等级：严重，漏洞评分：9.8。

ForgeRock AM 是一个开源的访问管理、权限控制平台，在大学、社会组织中存在广泛的应用。未经身份验证的攻击者可以通过构造特殊的请求远程执行任意代码，并接管运行 ForgeRock AM 的服务器。由于 ForgeRock AM 本身的权限管理功能，攻击者在控制 ForgeRock AM 的服务器还可以直接访问其他敏感服务，进行进一步的攻击。该漏洞不需要进行身份认证，无需任何用户交互，攻击成本低。同时因其为关键的边界身份认证服务，一旦遭到攻击，将导致非常严重的后果，利用价值极高。

对此，360CERT 建议广大用户及时将 ForgeRockAM 升级到最新版本。与此同时，请做好资产自查以及预防工作，以免遭受黑客攻击。

2 风险等级

360CERT 对该漏洞的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
攻击者价值	极高
利用难度	低
360CERT 评分	9.8

3 漏洞详情

3.1 CVE-2021-35464: ForgeRock AM 代码执行漏洞

CVE: CVE-2021-35464

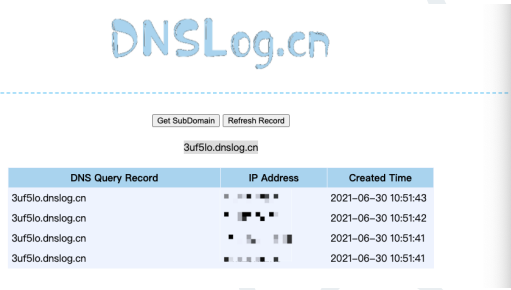
组件: ForgeRock AM

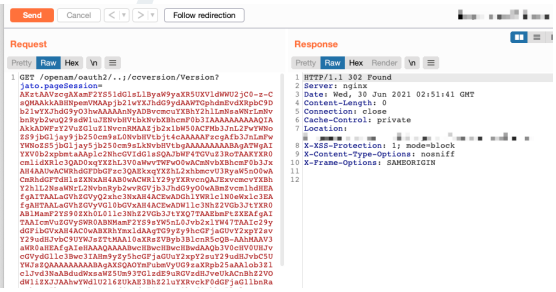
漏洞类型: 代码执行

影响: 服务器接管

简述: ForgeRock AM 中使用了 Jato 框架，该框架因历史原因已于 2005 年停止维护。在该框架中当处理 GET 请求参数jato.pageSession时会直接将其值进行反序列化。攻击者可以通过构造jato.pageSession值为恶意的序列化数据触发反序列化流程，最终导致远程代码执行。

360CERT 已经复现该漏洞:





4 影响版本

组件	影响版本	安全版本
ForgeRock AM	6.0.0.x	7
ForgeRock AM	6.5.0.x	7
ForgeRock AM	6.5.1	7
ForgeRock AM	6.5.2.x	7
ForgeRock AM	6.5.3	7

5 修复建议

5.1 通用修补建议

根据影响版本中的信息，排查并升级到安全版本

5.2 临时修复建议

1. 通过注释 AMweb.xml文件中的以下部分来禁止VersionServlet的映射

```
<servlet-mapping>
    <servlet-name>VersionServlet</servlet-name>
    <url-pattern>/ccversion/*</url-pattern>
</servlet-mapping>
```

2. 使用反向代理或者其他方法阻止对ccversion端点的请求。同时**避免出现通过反向代理进行 Tomcat 路径遍历的漏洞。**

6 时间线

2021-06-29 ForgeRock 官方发布安全通告

2021-06-29 portswigger 研究员发布分析报告

2021-06-30 360CERT 发布通告

7 参考链接

官方安全通告

Pre-auth RCE in ForgeRock OpenAM (CVE-2021-35464)

A 产品侧解决方案

若想了解更多产品信息或有相关业务需求，可移步至 http://360.net。

A.1 360 城市级网络安全监测服务

360CERT 的安全分析人员利用 360 安全大脑的 QUAKE 资产测绘平台 (quake.360.cn)，通过资产测绘技术的方式，对该漏洞进行监测。可联系相关产品区域负责人或 (quake#360.cn) 获取对应产品。

A.2 360 安全分析响应平台

360 安全大脑的安全分析响应平台通过网络流量检测、多传感器数据融合关联分析手段，对该类漏洞的利用进行实时检测和阻断，请用户联系相关产品区域负责人或 (shaoyulong#360.cn) 获取对应产品。

A.3 360 本地安全大脑

360 本地安全大脑是将 360 云端安全大脑核心能力本地化部署的一套开放式全场景安全运营平台，实现安全态势、监控、分析、溯源、研判、响应、管理的智能化安全运营赋能。360 本地安全大脑已支持对相关漏洞利用的检测，请及时更新网络神经元（探针）规则和本地安全大脑关联分析规则，做好防护。

A.4 360 终端安全管理系统

360 终端安全管理系统软件是在 360 安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全

产品。

360 终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控功能于一体的企业级安全产品。

360终端安全管理系统已支持对相关漏洞进行检测和修复，建议用户及时更新漏洞库并安装更新相关补丁。

B 报告等级说明

360CERT 评分是依托于 CVSS3.1 的评价体系，由 360CERT 进行分数评定的危害评分

严重	
评定标准	1. 9.0 ≤ 360CERT 评分 ≤ 10 2. Top20 组件 3. PoC/Exp 公开可直接利用 4. 获得系统权限 5. 蠕虫性攻击
危害结果	1. 实施攻击成本低，难度低 2. 直接获得服务器控制权限 3. 直接影响业务服务运行 4. 核心敏感数据泄漏 5. 下载任意文件 6. 易造成资金风险
修复建议	建议在 3 个工作日内对涉及的产品/组件进行修复操作

高危	
评定标准	1. 7.0 ≤ 360CERT 评分 < 9 2. 通用组件 3. PoC 公开 4. 获得服务/数据库权限
危害结果	1. 系统/服务/资源垂直越权 2. 获得数据库权限 3. 可造成资金风险
修复建议	建议在 7 个工作日内对涉及的产品/组件进行修复操作

中危	
评定标准	1. 4.0 ≤ 360CERT 评分 < 7 2. 需要额外的操作步骤方可实现攻击 3. 对服务的运行产生影响但不影响功能 (a) 占用存储空间 (b) 降低执行效率 4. 获得平台用户级权限
危害结果	1. 需要额外的操作步骤实现危害行为 2. 获得平台平行越权 3. 任意文件上传 4. 难造成资金风险
修复建议	建议在 12 个工作日内对涉及的产品/组件进行修复操作

低危	
评定标准	1. 0 ≤ 360CERT 评分 < 4 2. 不对服务的运行产生影响
危害结果	暂无
修复建议	建议在 20 个工作日内对涉及的产品/组件进行修复操作

C 影响面说明

影响面说明	
广泛	1. 影响主体数 > 10w 2. 底层依赖库
一般	1. 5w < 影响主体数 < 10w 2. 次级开源库
局限	1. 影响主体数 < 5w 2. 特制版本的

D 360CERT 内部评分体系

360 内部评分体系是 360CERT 安全研究人员经过一系列的数据分析和调查研究，并结合多年的漏洞研究经验最终得出的一套针对漏洞和安全事件的科学评分标准。此套评分体系能够用来评测漏洞和安全事件的严重程度，并帮助确定所需反应的紧急度和重要度。经验证，此评分体系适用于市面上几乎所有的漏洞和安全事件。

360 内部评分体系建立在"CVSS 漏洞评分体系"的基础上，其最终分数是取决于多个指标的公式，最终计算得出的近似的漏洞利用容易程度和漏洞利用的影响。分数范围是 0 到 10，其中最严重的是 10。该分数能较直观地反映漏洞的威胁等级，具体对应规则如下：

分数	威胁等级
9.0 –10.0	严重
7.0 –8.9	高危
4.0 –6.9	中危
0 –3.9	低危