安全事件通告

2020-10 补丁日: SAP 多个产品高危漏洞安全风险通告

360CERT
北京奇虎科技有限公司 | 2020-10-14

报告信息

报告名称	2020-10 补丁日: SAP 多个产品高危漏洞安全风险通告		
报告类型	安全事件通告	**报告编号**	B6-2020-101403
报告版本	1	**报告日期**	2020-10-14
报告作者	360CERT	**联系方式**	cert@360.cn
提供方	北京奇虎科技有限公司		
接收方			

报告修订记录

报告版本	日期	修订	审核	描述
1	2020-10-14	360CERT	360CERT	撰写报告

目录

一、事件档案

漏洞类型	代码执行漏洞
CVE 编号	CVE-2020-6296 等
相关厂商	Sap
相关组件	sap_solution_manager 等
威胁等级	严重
影响面	广泛
360CERT 评分	10
修复方案	通用修补方案
事件发布时间	2020-10-14
报告生成时间	2020-10-14

二、 事件简述

2020 年 10 月 14 日，360CERT 监测发现 SAP 官方 发布了 10 月份 安全更新的风险通告，事件等级：严重，事件评分：10。

SAP 于此次更新中，共计修复了 20 处安全漏洞。2 个严重漏洞，6 个高危漏洞。并对内置 Chromium 浏览器应用了最新的安全更新。

对此，360CERT 建议广大用户及时将 SAP 产品 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。

三、 事件评级

经过安全技术人员的分析，最终对该事件的评定结果如下

评定方式	等级
威胁等级	严重
影响面	广泛
360CERT 评分	10

四、 事件详情

CVE-2020-6364: 命令注入漏洞

SAP Solution Manager 和 SAP Focused Run 中存在一处命令注入漏洞。远程攻击者通过构造特制的数据包，发送到受影响的主机，可造成远程命令执行。该漏洞官方 CVSS 评分 10 分(10 分制)，360CERT 建议用户尽快对该漏洞进行补丁更新

CVE-2020-6296: 代码执行漏洞

SAP NetWeaver (ABAP) and ABAP Platform 中存在一处代码执行漏洞。远程攻击者通过构造特制的数据包，发送到受影响的主机，可造成远程代码执行。

SAP 内置 Chromium 安全更新

本次补丁日发布了针对 SAP 商业客户端内置的 Chromium 浏览器补丁更新。浏览器作为网络空间的第一入口，漏洞影响严重

五、 影响版本

产品名称	影响版本
sap_solution_manager	9.7/10.1/10.5/10.7
sap_focused_run	9.7/10.1/10.5/10.7

六、 安全建议

(一) 通用修补方案

SAP 为企业软件，请 SAP 的用户联系官方获取服务支持。

或访问并登录 SAP Support: https://support.sap.com/en/my-support.html

获得相关服务支持。

七、 产品侧解决方案

(一) 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。

八、 参考链接

1. SAP Security Patch Day – October 2020 - Product Security Response at SAP - Community Wiki

https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=558632196

附录 A 报告风险等级说明

360CERT 评分是依托 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. 任意攻击者可直接发起攻击 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

附录 B 影响面说明

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

附录 C 360 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