

# 漏洞事件通告

Incaseformat 蠕虫病毒威胁通告

360CERT

北京奇虎科技有限公司 | 2021-01-14

## 报告信息

报告名称	Incuseformat 蠕虫病毒威胁通告		
报告类型	漏洞事件通告	报告编号	B6-2021-011401
报告版本	1	报告日期	2021-01-14
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	2021-01-14	360CERT	360CERT	撰写报告

## 目录

一、	事件档案 .....	1
二、	事件简述 .....	2
三、	事件评级 .....	3
四、	安全建议 .....	4
	(一) 通用修补方案 .....	4
	(二) 临时修补方案 .....	4
五、	产品侧解决方案 .....	5
	(一) 360 安全卫士 .....	5
	(二) 360 安全分析响应平台 .....	5
六、	参考链接 .....	6
附录 A	报告风险等级说明 .....	7
附录 B	影响面说明 .....	9
附录 C	360 内部评分体系 .....	10

## 一、事件档案



漏洞类型	无类型
CVE 编号	暂无
相关厂商	Incuseformat
相关组件	Incuseformat
威胁等级	高危
影响面	广泛
360CERT 评分	8.5
修复方案	通用修补方案/临时修补方案
事件发布时间	2021-01-13
报告生成时间	2021-01-14

## 二、事件简述

---

2021年01月13日，360安全卫士发布了 Incaseformat 蠕虫病毒的风险通告，事件等级：高危，事件评分：8.5。

360第一时间发布了专杀工具与修复方案（见修复建议）

对此，360CERT建议广大用户好资产自查以及预防工作，以免遭受黑客攻击。

360CERT

### 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	高危
影响面	广泛
360CERT 评分	8.5

## 四、安全建议

---

### (一) 通用修补方案

360 安全卫士已支持对该病毒的查杀

用户可以通过安装 360 安全卫士或通过软件管家下载 incaseformat 专杀工具

### (二) 临时修补方案

1、文件不见了，空间占用正常

1) 不要重启，清空安全卫士信任区

2) 进行全盘杀毒

2、已经重启，或磁盘空间减少

1) 立即切断主机电源，并使硬盘断电

2) 向专业的数据恢复人员求助

## 五、产品侧解决方案

### (一) 360 安全卫士

针对本次安全更新，Windows 用户可通过 360 安全卫士实现对应补丁安装，其他平台的用户可以根据修复建议列表中的产品更新版本对存在漏洞的产品进行更新。如有其他问题可联系相关产品负责人或（360safe-ent#360.cn）。



### (二) 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。





## 六、 参考链接

---

1. 最新暴力蠕虫病毒“incaseformat”来袭！ 360 安全卫士轻松拿下！

<https://mp.weixin.qq.com/s/Mxl-ytdRBak67uq4PPww1A>

360CERT

## 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. $9.0 \leq 360\text{CERT 评分} \leq 10$ 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. $7.0 \leq 360\text{CERT 评分} < 9$ 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	<ol style="list-style-type: none"> <li>1. <math>4.0 \leq 360\text{CERT 评分} &lt; 7</math></li> <li>2. 需要额外的操作步骤方可实现攻击</li> <li>3. 对服务的运行产生影响但不影响功能                             <ol style="list-style-type: none"> <li>a) 占用存储空间</li> <li>b) 降低执行效率</li> </ol> </li> <li>4. 获得平台用户级权限</li> </ol>
危害结果	<ol style="list-style-type: none"> <li>1. 需要额外的操作步骤实现危害行为</li> <li>2. 获得平台平行越权</li> <li>3. 任意文件上传</li> <li>4. 难造成资金风险</li> </ol>
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	<ol style="list-style-type: none"> <li>1. <math>0 \leq 360\text{CERT 评分} &lt; 4</math></li> <li>2. 不对服务的运行产生影响</li> </ol>
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