

EMC远程备份恢复系统服务远程栈溢出漏洞 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/269/2021\\_2022\\_EMCC\\_E8\\_BF\\_9C\\_E7\\_A8\\_8B\\_E5\\_c67\\_269285.htm](https://www.100test.com/kao_ti2020/269/2021_2022_EMCC_E8_BF_9C_E7_A8_8B_E5_c67_269285.htm) BUGTRAQ ID: 25375

CVE(CAN) ID: CVE-2007-3618 EMC Legato NetWorker是一款跨平台的备份和恢复系统。EMC Legato NetWorker的远程Exec服务（nsrexecd.exe）存在栈溢出漏洞，远程攻击者可能利用此漏洞控制服务器。如果向poll或kill请求提交了超长的无效subcmd请求的话，就可以在对sprintf()的调用中触发这个溢出，导致执行任意指令。链接

: <http://marc.info/?l=bugtraq&w=2>

<http://secunia.com/advisories/26517/> \* > 建议：

----- 厂商补丁：

EMC --- 目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：

[http://www.emc.com/products/storage\\_management/navisphere.jsp](http://www.emc.com/products/storage_management/navisphere.jsp)

100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)