PCM蓄电池KF12-07 12V7AH/20HR系列参数

产品名称	PCM蓄电池KF12-07 12V7AH/20HR系列参数
公司名称	北京盛达绿能科技有限公司
价格	1.00/只
规格参数	品牌:PCM蓄电池 化学类型:免维护蓄电池 型号:KF12-07
公司地址	山东济南
联系电话	18053081797 18053081797

产品详情

PCM蓄电池KF12-07 12V7AH/20HR系列参数

另一项由调研机构波洛蒙研究所在今年10月发布的安全调查显示，有56%的公司表示缺乏可见性是造成数据泄露的主要原因。

一些IT团队由于担心会破坏原有的但对业务至关重要的系统而不想使用它们，有些团队没有资源来解决这些项目，也无法说服企业管理层将其作为头等大事。还有一些人可能根本不知道其基础设施中的遗留系统以及相关的风险。

Kennedy说，“ 我不认为企业董事会或管理人员了解这些遗留应用程序老化所带来的风险。但是众所周知的EternalBlue和WannaCry等网络攻击事件大多数针对的是旧版Windows操作系统的漏洞进行的。 ”

现在应该修复未损坏的内容

在安全性成为当今企业关注的焦点之前，已经创建了一些软件，有些是针对未暴露于公共互联网的环境而设计的。

总部位于休斯顿的网络安全厂商AlertLogic公司威胁情报产品副总裁RohitDhamankar表示，要解决此问题，需要深入研究应用程序，并添加所需的日志记录基础设施。

他表示，对于一些较旧的系统，初的开发人员可能已经离职，而对代码的处理可能会造成破坏。假设任务关键型应用程序由数据中心的一小部分人使用。如果初的开发人员离职，可能没有人会想采用这个软件。忽略原有操作系统的背后机制是相似的。由于升级操作系统可能会破坏正在运行的至关重要的应用程序，因此没有人愿意处理。这就是为什么在数据中心中仍使用许多过时的操作系统的部分原因。

他说，“ 大多数公司仍在使用到2020年不再支持其环境中的操作系统。人们仍然在2008年配置的Windows

服务器上运行程序。这是一个主要的问题，微软公司不会再提供补丁。用户没有任何东西可以保护正在构建的Microsoft应用程序堆栈。”而这里典型的是金融应用程序，老旧工资系统以及遗留Web应用程序。

Dhamankar说：“在Linux操作系统方面我们也有相同的看法。有些应用程序是在Apache或Jboss上构建的，但运行的Linux版本确实已过时了，例如Linux2.6版已经停止支持三年了。与此同时，这些操作系统可能具有已知的易于利用的严重漏洞。这就是数据中心经理正在处理的事情。”

Dhamankar表示，“摆脱遗留应用程序就像开展一个工程项目一样繁琐。需要重新构建应用程序或创建新的应用程序，并确保新功能在离开遗留应用程序之前可以正常工作。但这可能很难。很多人并不想重建已经存在的东西，例如旧版应用程序。此外，很多企业正在寻求投资回报率，或者关注是什么能够吸引更多的客户。如果数据中心或安全人员的工作能力不强，并且只向企业管理人员简单介绍业务案例，那么这些遗留项目往往不会获得资金支持。”

如果无法解决，需要缓解

遗留应用程序将会退出，但在此之前，数据中心管理可以采取一些措施来将风险降到。例如，如果遗留应用程序只被内部用户使用，那么它所在的系统应该被隔离。

Dhamankar建议说，“确保特定系统无法从互联网或不需要访问该系统的公司部门访问，以及确定哪些人可以访问遗留应用程序，这是采取的一些有效的缓解措施。”如果遗留应用程序需要互联网访问，则企业可以使用防火墙来阻止常见的攻击类型，例如SQL注入或跨站点脚本，或者应用白名单规则，以便只有一小部分经过批准的程序可以通过。也可以在主机系统上设置白名单。或者可以采用本地代理的形式，该代理仅允许遗留应用程序在该环境中运行，只能执行某些命令，而不能执行其他操作。

Dhamankar说，“但这可能有风险。如果遗留应用程序比较脆弱的话，那么在其环境中添加新功能(如日志记录或白名单)就有可能造成破坏。”

AttackIQ公司的Kennedy表示，在某些情况下，其他步骤可能包括购买对已停止使用操作系统的第三方支持，例如微软公司的扩展安全补丁支持。

归根结底，遗留应用程序的安全性问题不应仅由安全团队承担。

Illumio公司的Glenn说：“企业给安全监控中心(SOC)施加了太多压力，而对拥有遗留应用程序服务的人员却没有给予足够的压力。很明显在出了问题之后，安全团队有责任介入取证，但负责应用程序运行的是应用程序的所有者。为了了解这些应用程序如何工作并获取安全性所需的日志，这两个团队应该一起工作。”

他指出，“这些团队应该紧密结合，这是因为许多遗留应用程序通常都是关键的程序。”