(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112005232 A
(43)申请公布日 2020.11.27

(21)申请号 201880092927.9
(22)申请日 2018.08.20
(85)PCT国际申请进入国家阶段日
2020.10.29
(86)PCT国际申请的申请数据
PCT/US2018/047119 2018.08.20
(87)PCT国际申请的公布数据
WO2020/040731 EN 2020.02.27
(71)申请人 惠普发展公司,有限责任合伙企业
地址 美国德克萨斯州
(72)发明人 S·辛普森 H·麦克米兰
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 钟茂建 吕传奇
(51)Int.Cl.
G06F 21/50(2006.01)
G06F 21/57(2006.01)

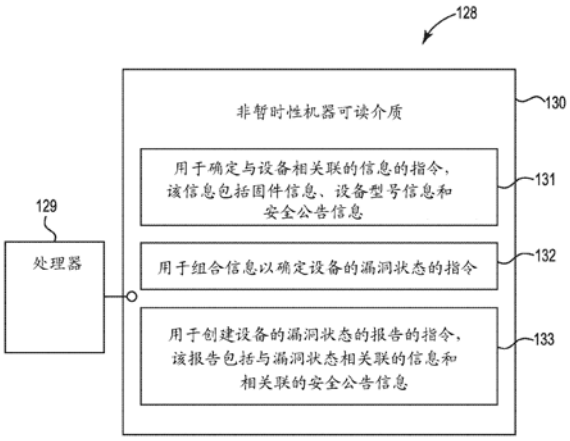
权利要求书2页 说明书6页 附图5页

(54)发明名称

漏洞状态报告

(57)摘要

示例实现涉及创建漏洞状态报告。示例非暂时性机器可读介质可以包括可执行以确定与设备相关联的信息的指令。该信息可以包括固件信息、设备型号信息和安全公告信息。示例非暂时性机器可读介质可以包括可执行以组合信息以确定设备的漏洞状态并创建设备的漏洞状态的报告的指令。该报告可以包括包括与漏洞状态相关联的信息和相关联的安全公告信息。



CN 112005232 A

1.一种非暂时性计算机可读介质,其包含指令,所述指令可由处理器执行以使处理器:

确定与设备相关联的信息,所述信息包括固件信息、设备型号信息和安全公告信息;

组合信息以确定设备的漏洞状态;以及

创建设备的漏洞状态的报告,所述报告包括与漏洞状态相关联的信息和相关联的安全公告信息。

2.根据权利要求1所述的介质,其中,可执行以组合信息以确定漏洞状态的指令包括可执行以将设备的多个漏洞状态中的一个优先化为设备的漏洞状态的指令。

3.根据权利要求1所述的介质,其中,漏洞状态包括:设备不具有与其相关联的已知安全公告、设备具有当前固件支持以及设备具有不多于一个过期的固件修订版。

4.根据权利要求1所述的介质,其中,漏洞状态包括:设备不具有与其相关联的已知安全公告、设备具有当前固件支持以及设备具有多个过期的固件修订版。

5.根据权利要求1所述的介质,其中,漏洞状态包括:设备不具有与其相关联的已知安全公告以及设备不具有当前固件支持。

6.根据权利要求1所述的介质,其中,漏洞状态包括:设备具有与其相关联的已知安全公告。

7.根据权利要求1所述的介质,其中,响应于设备不具有与其相关联的足够信息,漏洞状态包括未知漏洞状态。

8.一种控制器,包括与存储器资源通信的处理器,所述存储器资源包括指令,所述指令可执行以:

确定与多个设备相关联的信息,所述信息包括固件信息、设备型号信息和固件安全公告信息;

基于与多个设备相关联的信息,确定针对多个设备中的每一个设备的多个漏洞状态中的漏洞状态;以及

创建多个设备的可排序报告,所述报告包括多个设备中的每一个设备的漏洞状态、具有多个漏洞状态中的每一个漏洞状态的设备的百分比以及针对多个设备中的每一个设备的固件安全公告信息。

9.根据权利要求8所述的控制器,其中,多个设备包括多个打印设备。

10.根据权利要求8所述的控制器,其中:

设备型号信息进一步包括与设备型号的主动固件支持相关联的信息;以及

固件信息进一步包括与过期的固件修订版相关联的信息。

11.根据权利要求8所述的控制器,其中,可执行以确定固件安全公告信息的指令包括可执行以确定多个设备中的哪个具有与其相关联的固件安全公告的指令。

12.根据权利要求8所述的控制器,进一步包含可执行以经由图形用户界面显示报告的指令,所述显示包括:

多个设备的列表;以及

对于多个设备中的每一个设备:

相关联的固件安全公告的计数;

相关联的过期的固件修订版的数量;以及

当前设备支持状态。

13.一种方法,包括:

确定与多个设备中的每一个设备相关联的信息,所述信息包括:

是否主动支持多个设备中的每一个设备的固件;

多个设备中的每一个设备的固件修订版是否过期;以及

多个设备中的每一个设备是否具有与其相关联的固件安全公告;

基于与多个设备中的每一个设备相关联的信息的组合,针对多个设备中的每一个设备确定多个漏洞状态中的漏洞状态;

创建多个设备的报告,所述报告包括多个设备中的每一个设备的漏洞状态、具有多个漏洞状态中的每一个漏洞状态的设备的百分比以及针对多个设备中的每一个设备的固件安全公告信息;以及

经由图形用户界面显示报告,使得所述报告是交互式的并且是可按特定类别排序的。

14.根据权利要求13所述的方法,其中,确定多个设备中的每一个设备是否具有与其相关联的固件安全公告包括:将已知固件安全公告与特定固件版本相关联,所述特定固件版本与多个设备中的每一个设备相关联。

15.根据权利要求13所述的方法,进一步包括:

经由图形用户界面从用户接收请求,以按相关联的固件安全公告、过期固件修订版的数量或通用漏洞评分系统分数对报告进行排序;

响应于所述请求对所述报告进行排序;以及

经由图形用户界面显示排序的报告。

漏洞状态报告

背景技术

[0001] 固件是为设备的特定硬件提供低层控制的一类软件。固件可以被保存在非易失性存储设备中，所述非易失性存储设备诸如只读存储器(ROM)、可擦除可编程ROM(EPROM)或闪存。除了其他之外，包含固件的设备的示例还包括嵌入式系统、消费设备、打印设备、计算设备和计算设备外围设备。

附图说明

[0002] 图1图示了根据示例的用于创建漏洞(vulnerability)状态报告的系统；

图2图示了根据示例的包括处理器、存储器资源和引擎的控制器的图；

图3图示了根据示例的显示报告的图形用户界面(GUI)的显示；

图4图示了根据示例的显示报告的另一个GUI的显示；

图5图示了根据示例的显示报告的又一个GUI的显示；以及

图6图示了根据示例的用于创建漏洞状态报告的方法。

具体实施方式

[0003] 包括打印设备、计算设备和利用固件的其他设备的设备可能容易受到安全问题的影响，所述安全问题诸如网络漏洞或其他安全漏洞。更新固件可以解决这些漏洞，但消费者可能不知道过期的(out-of-date)固件、不支持的设备或与设备和/或固件相关联的固件安全公告。固件安全公告提供与特定固件(和/或软件)的版本相关联的漏洞的概要。除了其他之外，公告还可以由固件或设备提供商发布。除了其他漏洞、设备和固件信息之外，公告还可以包括关于受影响的固件版本、受影响的设备、可以被执行以修复漏洞的更新以及通用漏洞评分系统(CTSS)分数。

[0004] 解决固件漏洞的一些方法包括手动复查安全公告，并针对这些公告检查每个设备上的固件版本。这可能是耗时的，特别是对于具有大量设备的消费者来说，并且这也可能是容易出错的过程。其他方法包括将当前固件版本与最新可用固件版本进行比较的计划固件更新，以及响应于发现的新固件版本的更新。然而，这些方法不考虑当前是否支持特定的设备型号或固件可能有多少过期的修订版。此外，这些方法不基于安全公告信息、设备支持信息和过期修订版信息的组合来确定设备的漏洞状态。

[0005] 本公开的示例可以通过将安装在每个设备上的固件的版本与已知的漏洞进行比较来标识多个设备中的固件漏洞。例如，这可以通过标识是否主动支持谈论中的设备型号、标识相关联固件有多少过期修订版、以及通过基于是否有适用于该设备的公告、是否支持该设备型号以及针对该设备固件有多少过期的修订版来确定设备的漏洞状态来完成。

[0006] 本公开的一些示例可以组合来自多个源的信息，并基于该信息创建包括设备的漏洞状态的报告。该报告可以包括概要、关于每个设备的信息以及关于每个适用漏洞的信息。概要可以提供落入到不同漏洞类别中的设备的百分比的细分，并且设备信息可以包括针对每个设备的漏洞状态。适用的漏洞信息可以包括关于漏洞和受影响设备的详细信息。

[0007] 本公开的示例可以减少手动将设备固件版本与安全公告的列表进行比较的时间和错误。此外，可以提供包括当前是否支持固件和/或设备的上下文，以及包括固件的过期修订版的数量的上下文。附加的上下文可以创建更鲁棒的漏洞状态报告，并且可以有助于固件更新决策制定。

[0008] 图1图示了根据示例的用于创建漏洞状态报告的系统128。在一些示例中，系统128可以是计算设备并且可以包括处理器129。系统128可以进一步包括非暂时性机器可读介质(MRM)130，可以在所述非暂时性机器可读介质(MRM)130上存储指令，诸如指令131、132和133。尽管以下描述涉及处理器和存储器资源，但是所述描述也可以适用于具有多个处理器和多个存储器资源的系统。在这样的示例中，指令可以跨多个非暂时性MRM分布(例如，存储)，并且指令可以跨多个处理器分布(例如，由其执行)。

[0009] 非暂时性MRM 130可以是电子、磁性、光学或存储可执行指令的其他物理存储设备。因此，非暂时性MRM 130可以是例如随机存取存储器(RAM)、电可擦除可编程ROM(EEPROM)、存储驱动器、光盘以及诸如此类，暂时性MRM 130上可以被布置在系统128内，如图1中所示。在该示例中，可执行指令131、132和133可以被“安装”在设备上。附加地和/或替代地，非暂时性MRM 130可以是例如便携式、外部或远程存储介质，其允许系统128从便携式/外部/远程存储介质下载指令131、132和133。在这种情况下，可执行指令可以是“安装包”的部分。如本文中所描述的那样，非暂时性MRM 130可以编码有用于漏洞状态报告创建的可执行指令。

[0010] 当由诸如处理器129的处理器执行时，指令131可以包括用于确定与设备相关联的信息的指令，该信息包括固件信息、设备型号信息和安全公告信息。例如，除了其他之外，固件信息还可以包括版本名称、版本、日期和产品系列。除了其他之外，设备型号信息还可以包括型号名称、产品系列以及是否支持设备型号。除了其他之外，安全公告信息还可以包括标识符、描述、URL、受影响的设备型号和受影响的固件版本。可以确定与设备相关联的其他信息，该信息例如包括设备型号编号/名称、序列号、固件版本和客户信息。

[0011] 当由诸如处理器129的处理器执行时，指令132可以包括用于组合信息以确定设备的漏洞状态的指令。例如，与设备相关联的前述信息可以被用于确定每个设备的漏洞状态。例如，漏洞状态可以包括“正常”状态，其包括不具有与其相关联的已知安全公告的设备、具有当前固件支持的设备以及具有不多于一个过期的固件修订版的设备。

[0012] 不同的漏洞状态可能是“过期”状态。这可以包括不具有与其相关联的已知安全公告的设备、具有当前固件支持的设备以及具有多个过期的固件修订版的设备。“被动支持(reactive support)”漏洞状态可以包括不具有与其相关联的已知安全公告的设备以及不具有当前固件支持的设备。

[0013] 在一些示例中，“公告”漏洞状态可以包括具有与其相关联的已知安全公告的设备，并且“未评估”漏洞状态可以包括其中漏洞状态是未知的和/或无法基于不具有与其相关联的足够信息的设备来确定的情况。例如，用户可能已经将设备型号编号改变为无法标识和/或验证的不可识别的名称或编号。虽然这里使用“正常”、“过期”、“被动支持”、“公告”和“未评估”，但是可能向漏洞状态分配其他名称，并且可能使用更多或更少的漏洞状态。

[0014] 在一些示例中，设备可以具有多于一个漏洞状态和/或具有重叠的漏洞状态。例如，设备可以具有与其相关联的安全公告，但也受到支持并具有一个过期的固件修订版。该

示例可能落入到“公告”状态中，但也与“正常”状态重叠。在这样的示例中，设备的多个漏洞状态中的一个可以相对于另一个被优先化为设备的漏洞状态。例如，因为“公告”状态比“正常”状态更严重，所以“公告”状态可以相对于“正常”状态被优先化。在一些示例中，可以基于严重性对漏洞状态进行优先化，其中严重性的次序(从最严重到最不严重)是“公告”、“不支持(out-of-support)”、“被动支持”和“正常”。然而，优先化不限于这种排序。

[0015] 当由诸如处理器129之类的处理器执行时，指令133可以包括用于创建设备的漏洞状态的报告的指令，该报告包括与漏洞状态相关联的信息和相关联的安全公告信息。例如，报告可以包括关于设备的信息(例如，序列号、产品名称、当前固件版本、最新可用的固件版本等)、其相关联的漏洞状态(例如，过期的修订版、相关联的公告的数量、被动支持状态等)以及公告信息(例如，相关联的公告的数量、到相关安全公告的链接等)。

[0016] 在一些情况下，报告可以包括关于与客户相关联的多个设备(诸如打印设备)的信息。例如，客户可能具有多个打印设备，并且报告可以说明每个打印设备的漏洞状态。在一些示例中，客户或其他用户可以经由GUI查看报告并可以与报告进行交互。例如，客户或其他用户可以选择基于与多个打印设备相关联的过期的修订版的数量对报告进行排序。

[0017] 图2图示了根据示例的包括处理器218、存储器资源221以及引擎222、223和224的控制器220的图。例如，控制器220可以是用于漏洞状态报告创建的硬件和指令的组合。硬件例如可以包括处理器218和/或存储器资源221(例如，MRM、计算机可读介质(CRM)、数据存储等)。

[0018] 如本文中所使用的那样，处理器218可以包括能够执行由存储器资源221存储的指令的多个处理资源。指令(例如，机器可读指令(MRI))可以包括存储在存储器资源221上并且可由处理器218执行以实现期望功能(例如，创建漏洞状态报告)的指令。如本文中所使用的那样，存储器资源221可以包括能够存储可以由处理器218执行的非暂时性指令的多个存储器组件。存储器资源221可以被集成在单个设备中或跨多个设备分布。此外，存储器资源221可以与处理器218完全或部分地集成在相同设备中，或者其可以是分离的但是对于该设备和处理器218而言可访问的。因此，注意，除了其他可能性之外，控制器220还可以在电子设备和/或电子设备的集合上实现。

[0019] 存储器资源221可以经由通信链路(例如，路径)219与处理器218通信。通信链路219相对于与处理器218相关联的电子设备可以是本地的或远程的。存储器资源221包括引擎(例如，信息引擎222、漏洞引擎223和报告引擎224)。存储器资源221可以包括比图示更多的引擎以执行本文中描述的各种功能。

[0020] 引擎222、223和224可以包括硬件和指令的组合以执行本文中描述的多个功能(例如，创建漏洞状态报告)。除了其他可能性之外，指令(例如，软件、固件等)还可以被下载并存储在存储器资源(例如，MRM)以及硬连线程序(例如，逻辑)中。

[0021] 信息引擎222可以确定与多个设备相关联的信息。例如，该信息可以包括固件信息、设备型号信息和固件安全公告信息。设备型号信息可以包括与设备型号的主动固件支持相关联的信息，并且固件信息可以包括与过期的固件修订版相关联的信息。例如，该确定可以包括是否主动地支持该设备型号(例如，如果该设备及其固件是旧的并且不再主动地支持)以及有多少过期的固件修订版与该设备相关联。

[0022] 在一些示例中，确定信息可以包括从多个数据库获取(harvest)信息，该数据库包

括具有针对每个设备的型号标识符、序列号和固件版本的设备列表。该确定还可以包括按程序将产品分组(例如,相关产品、运行相同固件的产品等)和/或确定多个设备中的每一个设备属于哪个程序。使用该信息,可以做出关于是否主动更新程序(例如,是否主动更新固件)或者是否不再支持该程序的确定。在一些情况下,确定信息可以包括收集关于如何更新固件的信息。

[0023] 在一些示例中,确定固件安全公告信息包括确定多个设备中的哪个具有与其相关联的固件安全公告。例如,可以做出关于哪些公告影响哪些设备的确定。例如,如果客户具有设备A、B和C,则可以确定多个固件安全公告中的哪个(如果有的话)影响设备A、B和C中的任何或所有。换句话说(Out another way),固件安全公告可以与特定的固件版本相关联,该特定的固件版本与特定的设备关联。

[0024] 漏洞引擎223可以基于与多个设备相关联的信息来确定针对多个设备中的每一个设备的多个漏洞状态中的漏洞状态。例如,使用包括主动固件支持信息、过期固件修订版信息和固件安全公告信息的信息,可以确定漏洞状态。在一些示例中,可以根据诸如“正常”、“过期”、“被动支持”、“公告”和“未评估”的多个状态确定漏洞状态,如参考图1所描述的那样。在一些示例中,另一个漏洞状态可以包括“无数据”,其中特定设备上的数据尚未被收集和/或是不可用的。

[0025] 报告引擎224可以创建多个设备的可排序报告,该报告包括多个设备中的每一个设备的漏洞状态、具有多个漏洞状态中的每一个漏洞状态的设备的百分比以及针对多个设备中的每一个设备的固件安全公告信息。例如,报告可以包括在确定漏洞状态时考虑的因素。报告可以是可排序的,使得除了其他之外用户还可以基于漏洞状态、公告、设备的位置和CVSS分数对他或她的漏洞状态结果进行排序。

[0026] 例如,如果用户在世界各地的多个位置中具有数千个计算设备和/或打印设备,则排序选项对于确定哪些区域需要更新和/或哪些特定设备需要更新可能是有益的。如与针对固件安全公告手动检查数千个设备中的每一个设备相比,这可以导致时间和成本节省。此外,手动检查不考虑诸如主动固件支持、过期固件修订版和固件安全公告的因素的组合。

[0027] 在一些示例中,报告可以经由GUI显示,并且显示可以包括多个设备的列表。对于多个设备之一中的每个,可以显示相关联的固件安全公告的计数、相关联的过期固件修订版的数量以及当前设备支持状态。相关联的固件安全公告的计数可以包括与该特定设备上的固件相关联的固件安全公告的数量(例如,0、1、2等)。这可能有助于确定固件的立即更新有多重要(例如,作为漏洞状态确定的一部分)。

[0028] 相关联的过期固件修订版的数量可能包括有多少修订版已经被设备错过和/或未在设备上实现。例如,如果设备落后两个修订版,则它可能具有两个相关联的过期的固件修订版。过期的固件修订版的数量越大,设备的风险就越大。当前设备支持状态可以包括当前是否支持设备和/或其固件的确定。如果否(例如,设备非常旧),则安全问题的风险增加,如漏洞状态严重性增加一样。

[0029] 在一些情况下,显示的报告可以允许由用户进行交互,包括前述报告的排序。报告的可视化可以说明哪些设备和固件处于安全问题的最高风险处。这可以鼓励用户更新固件。此外,它可以允许用户看到他们的设备的状态,如与其他安全问题检测方法相比,这可以导致时间和成本节省。在一些情况下,连同相关联的固件安全公告计数一起,超链接可以

是经由GUI可获得的，以将用户链接到(一个或多个)相关联的安全公告。

[0030] 图3图示了根据示例的显示报告的GUI的显示300。在310处，用户可以输入客户名称(例如，“客户A”)，并且可以显示客户的设备漏洞状态301、302、303、304、305和306的概要。每个漏洞状态301、302、303、304、305和306都可以包括相关联的描述，以及具有该特定漏洞状态的设备的数量和具有该漏洞状态的总设备的百分比。例如，“公告”漏洞状态304包括具有有与其相关联的已知安全公告的固件的设备。客户A具有33个具有“公告”漏洞状态304的设备，其占166个总设备的20％(例如，如307处图示的那样)。饼图311图示了设备中的每个以及相关联的漏洞状态301、302、303、304、305和306的细分百分比。

[0031] 在一些示例中，可以在308处将结果按地区排序或在309处按国家排序。例如，如果客户A在多个国家中具有设备，则他或她可能希望按国家排序，以确定他的设备例如在美国或加拿大的漏洞状态。在一些情况下，客户A可能在美国内有地区，并且他或她可能希望基于中西部地区对结果进行排序，以确定那些设备中的哪些可能准备好固件升级。

[0032] 图4图示了根据示例的显示报告的另一GUI的显示412。类似于图3的显示300，用户可以在410处输入客户信息。作为响应，显示412可以包括415处的漏洞状态的详细报告、417处的设备以及在416处的它们的相关联的序列号、418处的相关联的当前固件版本、419处的最新固件版本、425处的过期的相关联的固件修订版的数量、426处的相关联的公告计数、427处的被动支持状态、435处的相关联的国家以及436处的相关联的地区。例如，设备X具有“公告”的漏洞状态和序列号A。设备X的当前固件版本为1，并且最新固件版本为2。设备X具有3个过期的固件修订版和一个相关联的固件安全公告。被动支持状态为空(null)，意指支持设备X(状态为“真”可以指示不支持设备)。设备X位于EMEA地区中的英国内。

[0033] 如图4中所图示的那样，诸如客户A的客户可以具有多个相同的设备(例如，设备Y)，使得它在报告中被图示多次。对于相同的设备，漏洞状态415以及其他方面是相同的。在一些示例中，显示412的结果可以在413处按漏洞状态、在414处按过期固件修订版的阈值数量、在408处按地区或在409处按国家来排序。

[0034] 图5图示了根据示例的显示报告的又一个GUI的显示537。在512处，用户可以输入客户名称，并且可以生成关注于固件安全公告的报告。例如，对于542处的每个设备，可以连同541处的设备序列号、543处的当前设备固件版本、544处的解析的固件版本、545处的最新的固件版本、546处的国家、547处的地区、549处的CVSS以及548处的安全公告标识符一起，在540处显示漏洞状态。例如，设备Q具有序列号C和漏洞状态“公告”，当前相关联的固件版本是6，而解析的固件版本是10，并且最新的固件版本是14。产品Q位于EMEA地区中的英国内。产品Q也与公告123相关联，并且具有6.8的CVSS分数。CVSS分数是公告中提供的标准化分数，用于对影响固件的安全风险/重要性进行分类。在一些示例中，栏548可以包括到与多个设备中的每一个设备相关联的特定公告的超链接。

[0035] 在一些情况下，显示537的报告中的结果可以在508处按地区排序，或者在509处按国家排序。在538处，可以按固件安全公告(例如，可以做出关于要显示哪个(哪些)公告的选择)或在539处按CVSS分数来对结果进行排序。例如，较高的CVSS分数可能指示大的风险，因此通过按高分数排序，可以确定哪些设备风险最大，并可以首先对其进行更新以解决漏洞。

[0036] 图6图示了根据示例的用于创建漏洞状态报告的方法660。在662处，方法660可以包括确定与多个设备中的每一个设备相关联的信息。该信息可以包括例如是否主动支持多

个设备中的每一个设备的固件、多个设备中的每一个设备的固件修订版是否过期以及多个设备中的每一个设备是否具有与其相关联的固件安全公告。

[0037] 在一些示例中，确定多个设备中的每一个设备是否具有与其相关联的固件安全公告可以包括已知固件安全公告与特定固件版本相关联，所述特定固件版本与多个设备中的每一个设备相关联。例如，可以做出关于哪些公告影响哪些固件版本的确定，并且作为响应，可以做出关于客户是否具有与那些固件版本相关联的设备的确定。

[0038] 在664处，方法660可以包括基于与多个设备中的每一个设备相关联的信息的组合，针对多个设备中的每一个设备确定多个漏洞状态中的漏洞状态。例如，使用前述信息，基于漏洞状态准则，可以将漏洞状态分配给每个设备。例如，如果设备及其相关联的固件不具有与其相关联的已知安全公告，但是未主动支持该固件，则该设备可以被给予“被动支持”漏洞状态。如先前指出的那样，其他漏洞状态可以包括(但不限于)“正常”、“过期”、“公告”、“未评估”和“无数据”。

[0039] 在666处，方法660可以包括创建多个设备的报告。该报告可以包括多个设备中的每一个设备的漏洞状态、具有多个漏洞状态中的每一个漏洞状态的设备的百分比以及针对多个设备中的每一个设备的固件安全公告信息。例如，该报告可以包括概要(例如，如图3中所图示的那样)、关于每个设备的详细信息(例如，如图4中所图示的那样)和/或关于每个漏洞状态和/或固件安全公告的详细信息(例如，如图5中所图示的那样)。

[0040] 在668处，方法660可以包括经由GUI显示报告，使得报告是交互式的并且是可按特定类别排序的。例如，显示可以是交互式的，使得用户可以输入客户信息并且除了其他之外还按诸如漏洞状态、地区、国家、过期的固件修订版、公告和CVSS分数的类别对报告结果进行排序。换句话说，可以经由GUI从用户接收请求，以按相关联的固件安全公告、过期固件修订版的数量或CVSS分数对报告进行排序。可以响应于请求来对报告进行排序，并且可以经由GUI显示排序的报告。

[0041] 这样的显示可以提供用于更新固件的动机。例如，可以使用多个类别来确定设备漏洞分数，包括过期的固件修订版和主动支持状态，如与不考虑这些的方法相比，这可以导致更准确的漏洞预测。例如，类别可以被组合并转换为针对特定设备的漏洞状态。用户可以使用这些预测和漏洞状态来确定哪些设备可以在特定时间被更新。如与不这么详细并且不允许基于多个类别的报告的其他方法相比，这可以减少用于更新和调查漏洞的时间和成本。

[0042] 在本公开的前述详细描述中，参考了形成其一部分的附图，并且其中通过图示的方式示出了可以如何实施本公开的示例。足够详细地描述这些示例，以使得本领域中的普通技术人员能够实施本公开的示例，并且要理解，在不脱离本公开的范围的情况下，可以利用其他示例，并且可以进行过程、电气和/或结构改变。

[0043] 本文中的附图遵循编号惯例，其中第一个数字对应于附图编号，并且其余数字标识附图中的元素或组件。可以添加、交换和/或消除本文中各图中所示的元素，以便提供本公开的多个附加示例。此外，附图中提供的元素的比例和相对尺度旨在图示本公开的示例，并且不应以限制性意义来理解。此外，如本文中所使用的那样，“多个”元素和/或特征可以指代这样的元素和/或特征中的一个或多个。

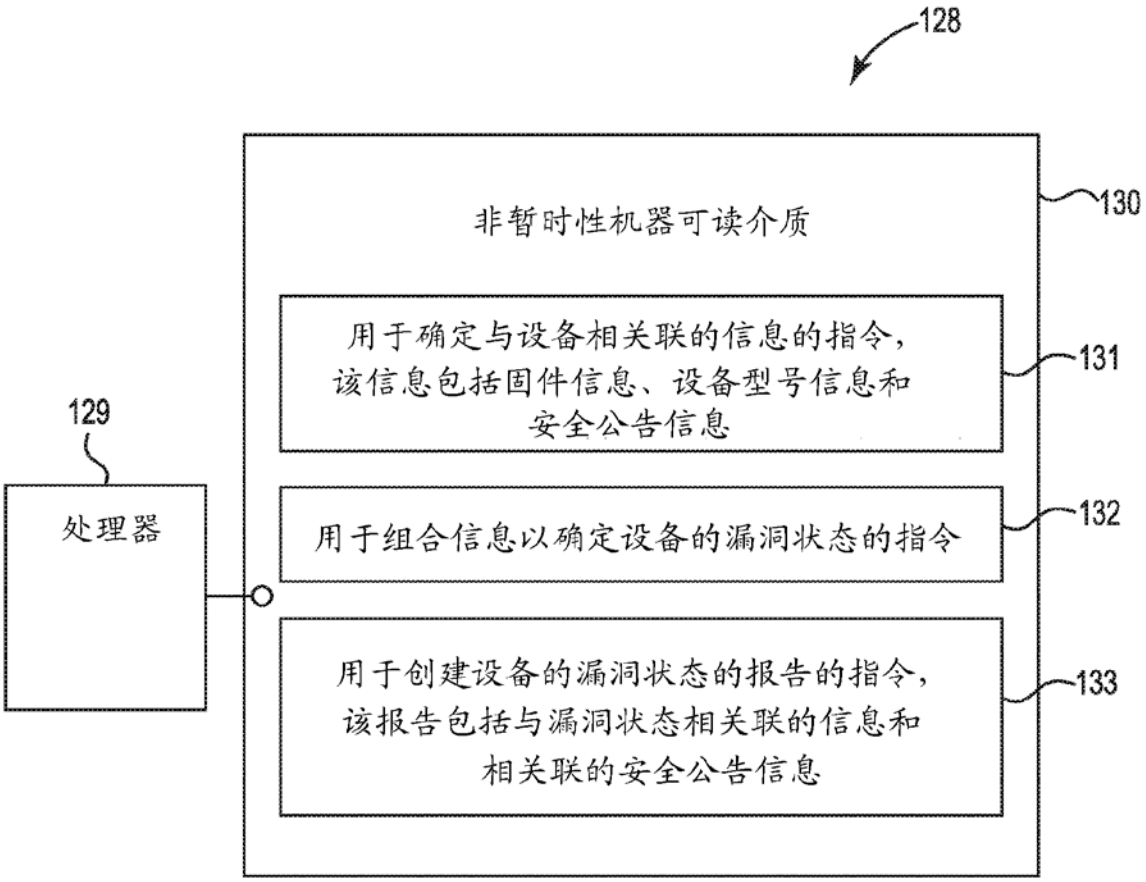

128
非暂时性机器可读介质
130
用于确定与设备相关联的信息的指令，该信息包括固件信息、设备型号信息和安全公告信息
131
129
处理器
用于组合信息以确定设备的漏洞状态的指令
132
用于创建设备的漏洞状态的报告的指令，该报告包括与漏洞状态相关联的信息和相关联的安全公告信息
133

图 1

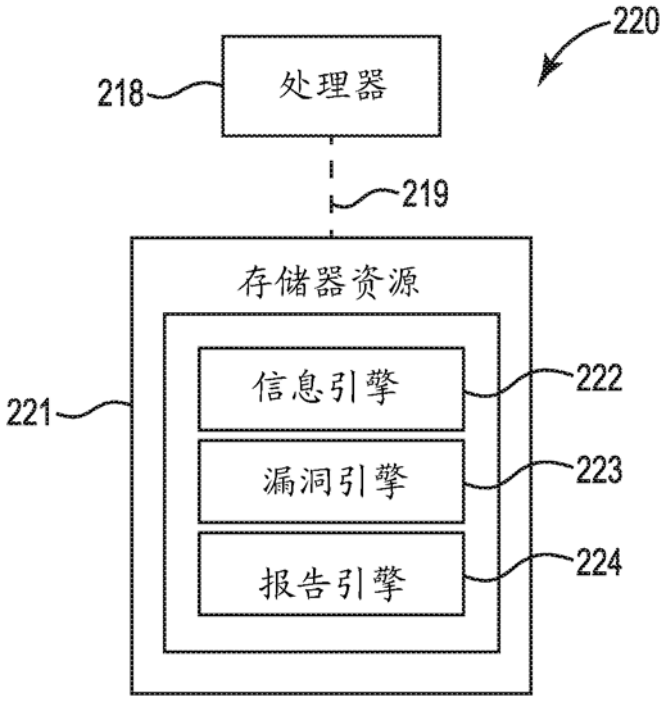

220
218
处理器
219
存储器资源
221
信息引擎
222
漏洞引擎
223
报告引擎
224

图 2

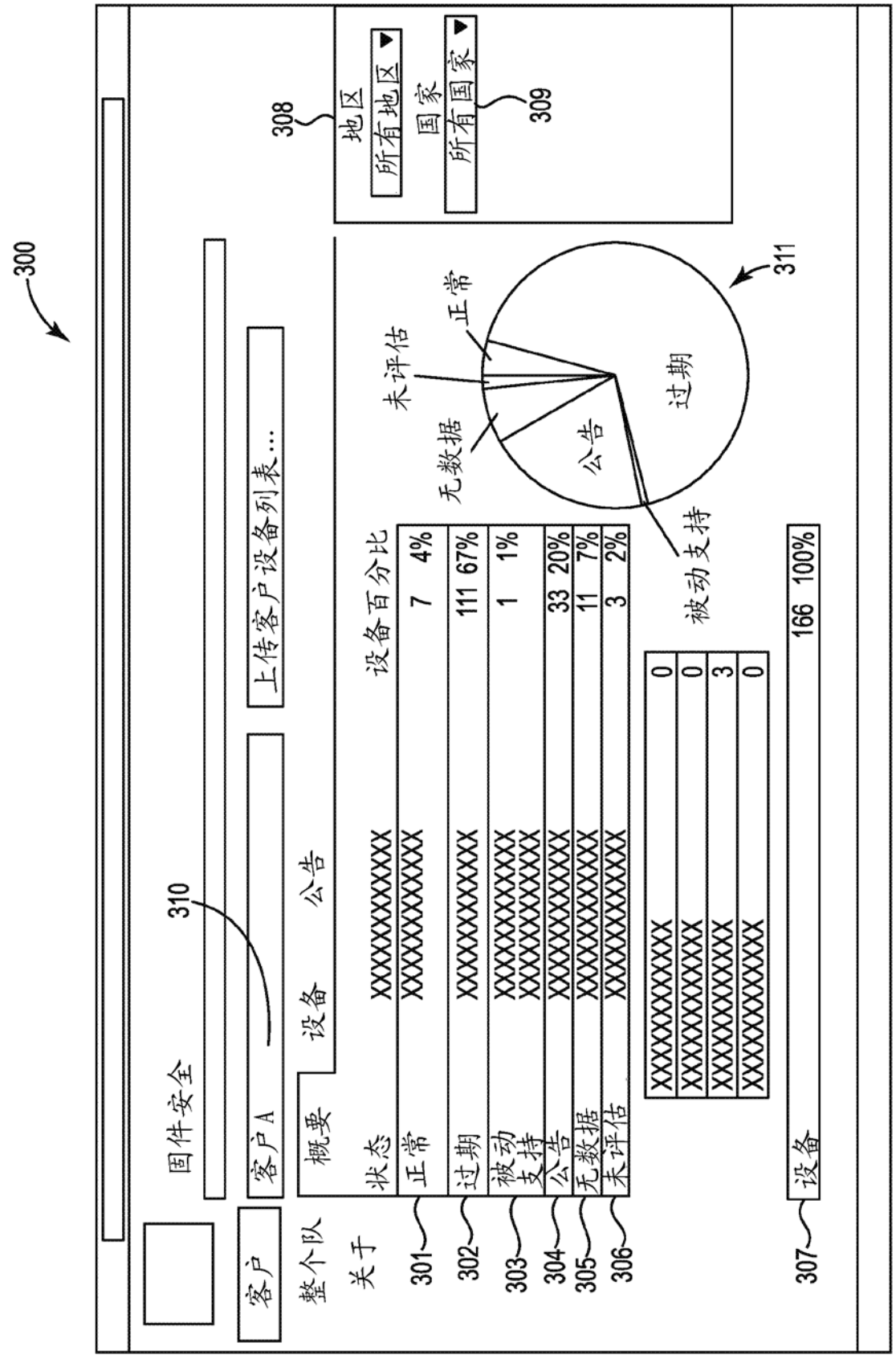

300
固件安全
客户
客户A
上传客户设备列表...
概要
设备
公告
整个队
关于
310
308
地区
所有地区
国家
所有国家
309
311
状态
设备百分比
正常 7 4%
过期 111 67%
被动支持 1 1%
公告 33 20%
无数据 11 7%
未评估 3 2%
XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX
0
0
3
0
166 100%
设备
正常
过期
公告
无数据
未评估
被动支持
301
302
303
304
305
306
307

图 3

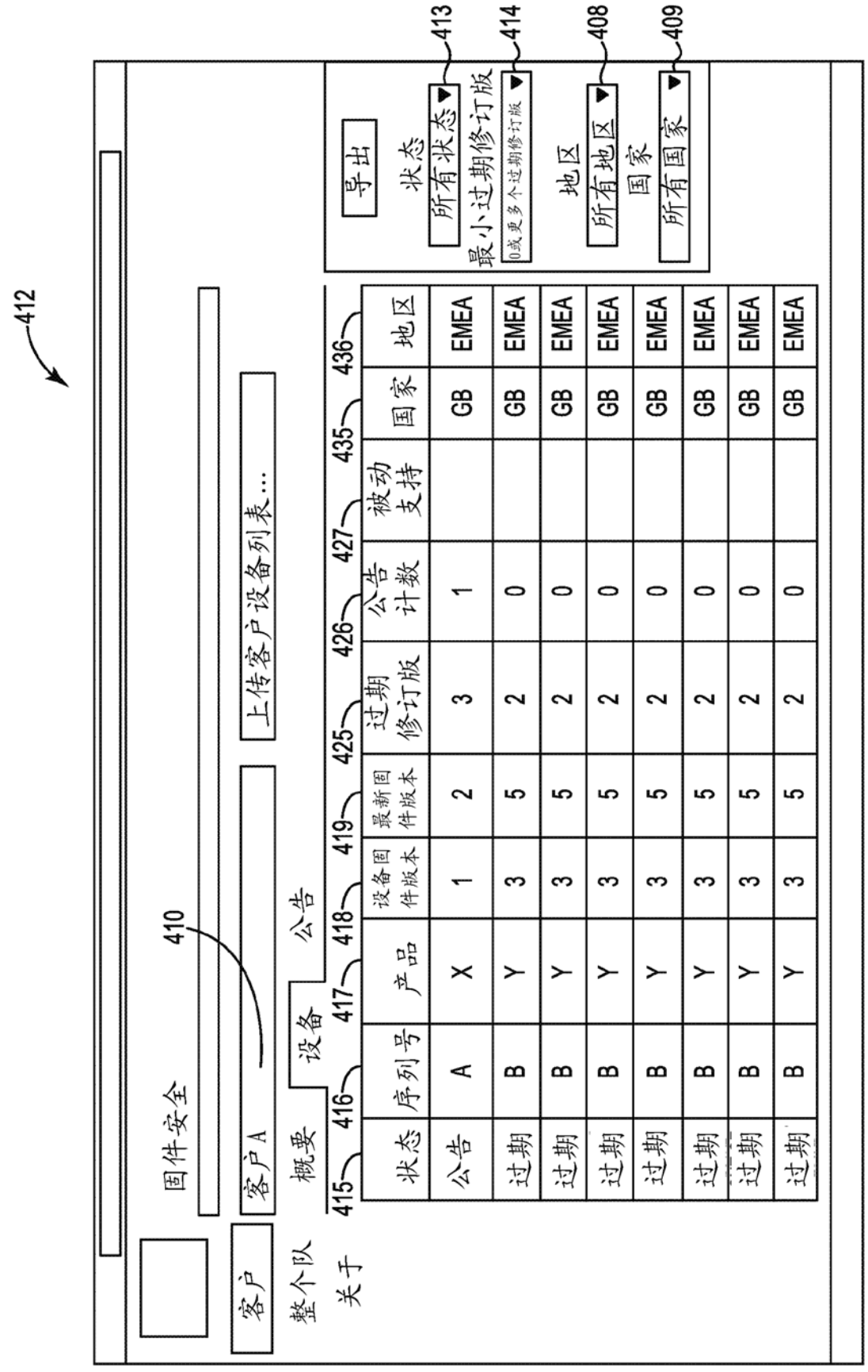

412
410
固件安全
客户A
上传客户设备列表...
客户
整个队
关于
概要
设备
公告
导出
状态
所有状态
最小过期修订版
0或更多个过期修订版
地区
所有地区
国家
所有国家
413
414
408
409
415
416
417
418
419
425
426
427
435
436
状态
序列号
产品
设备固件版本
最新固件版本
过期修订版
公告计数
被动支持
国家
地区
公告 A X 1 2 3 1 GB EMEA
过期 B Y 3 5 2 0 GB EMEA
过期 B Y 3 5 2 0 GB EMEA
过期 B Y 3 5 2 0 GB EMEA
过期 B Y 3 5 2 0 GB EMEA
过期 B Y 3 5 2 0 GB EMEA
过期 B Y 3 5 2 0 GB EMEA
过期 B Y 3 5 2 0 GB EMEA

图 4

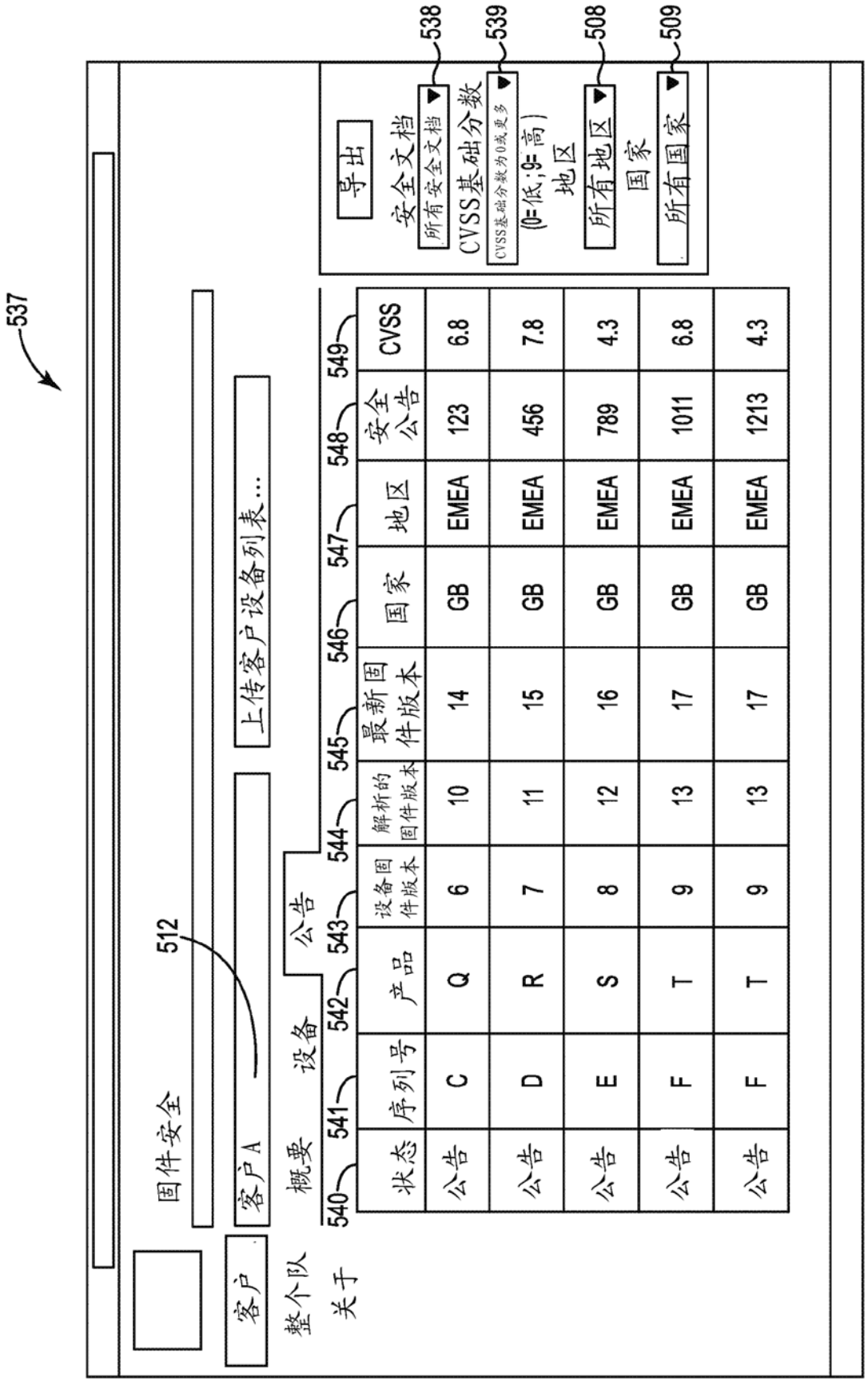

537
固件安全
512
客户A
上传客户设备列表...
客户
整个队
关于
概要
设备
公告
寻出
安全文档
所有安全文档
538
CVSS基础分数
CVSS基础分数为0或更多
539
(0=低;9=高)
地区
所有地区
508
国家
所有国家
509
状态 541 序列号 542 产品 543 设备固件版本 544 解析的固件版本 545 最新固件版本 546 国家 547 地区 548 安全公告 549 CVSS
公告 C Q 6 10 14 GB EMEA 123 6.8
公告 D R 7 11 15 GB EMEA 456 7.8
公告 E S 8 12 16 GB EMEA 789 4.3
公告 F T 9 13 17 GB EMEA 1011 6.8
公告 F T 9 13 17 GB EMEA 1213 4.3
540

图 5

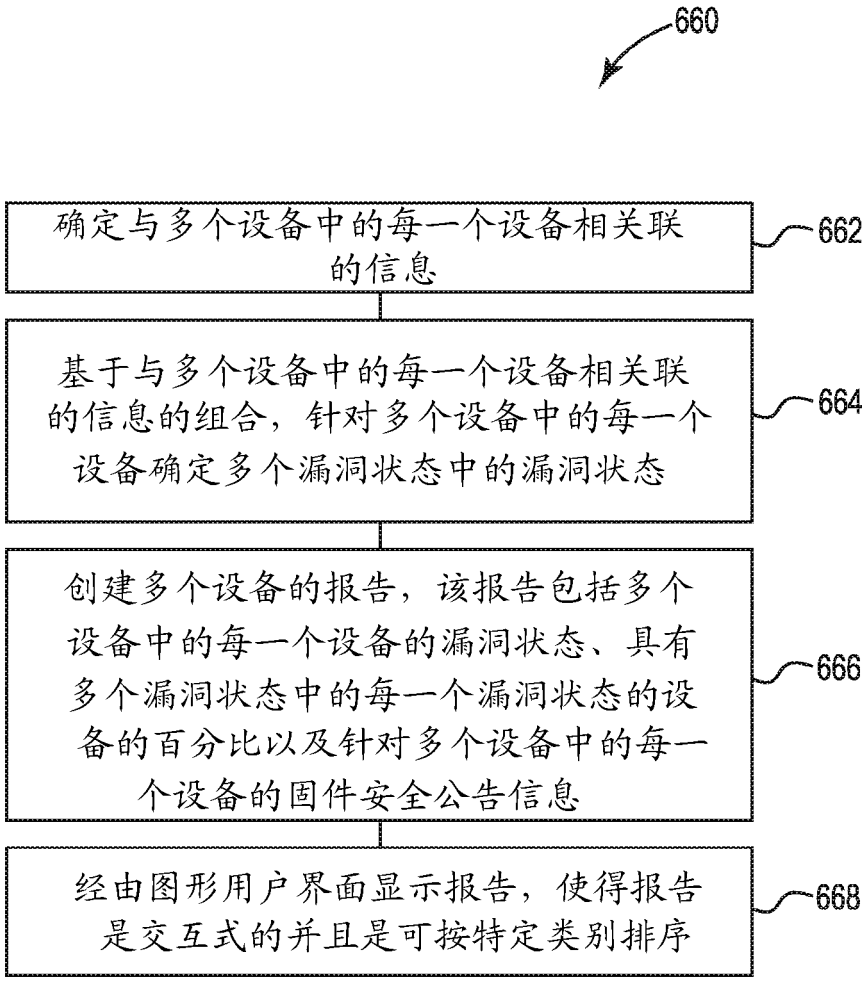

660
确定与多个设备中的每一个设备相关联的信息
662
基于与多个设备中的每一个设备相关联的信息的组合，针对多个设备中的每一个设备确定多个漏洞状态中的漏洞状态
664
创建多个设备的报告，该报告包括多个设备中的每一个设备的漏洞状态、具有多个漏洞状态中的每一个漏洞状态的设备的百分比以及针对多个设备中的每一个设备的固件安全公告信息
666
经由图形用户界面显示报告，使得报告是交互式的并且是可按特定类别排序
668

图 6