苹果曝出严重安全漏洞 相当于给了黑客一把万能钥匙?

本报记者 李玉洋 李正豪 上海报道

iPhone14即将发布,0day(在网络安全界通常是指没有补丁的漏洞利用程序)级别漏洞盖在了苹果头上。

近日,苹果公司被曝出旗下的手机、平板、电脑等硬件产品存在严重安全漏洞,而这些漏洞可以让黑客轻松获得设备的"完全管理权限",并以他们的名义运行任何软件。目前苹果并未对外透露该漏洞的更多详情,仅表示是由一名匿名研究人员发现了这一漏洞。

"0day级别漏洞是说刚刚被发现、还没有被公开的漏洞,威胁很大。"民间互联网安全组织网络尖刀安全团队成员沦沦告诉《中国经营报》记者,鉴于苹果自身很注重安全漏洞方面的问题,出现0day级别漏洞实属"比较少见",但该漏洞还不是天花板级别,建议苹果用户及时升级系统。

360漏洞研究院人士也向记者表示,这次漏洞影响非常广泛,几乎影响苹果所有的设备,如iPhone、iPad、Mac等,但"从历史攻击事件来看,针对苹果设备的攻击主要集中在特定的高价值人群或者某些特定组织,所以对普通用户来说,及时更新系统,不随意点击未知的链接,还不需要太过于紧张"。

对于此次漏洞是否已被利用、造成损失以及将来如何应对类似漏洞等问题,记者联系苹果中国方面,截至发稿未获答复。不过目前苹果公司公开声称已经找到相应的解决方法,同时呼吁用户立刻下载最新更新,以修补漏洞。

苹果曝出严重安全漏洞,黑客可全面接管设备。 视觉中国/图

漏洞已被利用

"目前国内已经有多个安全团队发现该漏洞已经被利用的情况,即外部已有攻击组织在利用这类漏洞。"

据了解,受本次漏洞影响的设备涵盖了手机、平板、电脑"苹果三件套":手机包括iPhone 6S及以后的型号;平板包括第五代及以后的iPad、所有的iPad Pro以及iPad Air 2;电脑则是运行MacOS Monterey的Mac。此外,该漏洞还能影响到部分型号的iPod。

"我们从公开的信息看,该漏洞主要利用的是Apple WebKit代码执行漏洞(CVE-2022-32893)和Apple Kernel权限提升漏洞(CVE-2022-32894)。"沦沦表示,Apple Webkit是浏览器引擎,被使用在Safari、Mail、App Store、iOS和Linux,Apple Webkit在处理恶意制作的Web内容可能会导致任意代码执行,简单来说,Apple内核存在本地权限提升漏洞,"通过越界读写,成功利用该漏洞可以将本地用户权限提升至内核权限,并以内核权限执行任意代码"。

需要指出的是,CVE指的是通用漏洞披露(Common Vulnerabilities and Exposures)。对于该漏洞的解析,深度科技研究院院长张孝荣则形象地称之为相当于给了黑客一把万能钥匙,随时可以出入用户的终端。

沦沦还表示,目前国内已经有多个安全团队发现该漏洞已经被利用的情况,即外部已有攻击组织在利用这类漏洞。"目前看各大安全厂商的反馈(该漏洞)还没有大范围扩散,漏洞细节也还未进行公开。"他说。

在所发布的安全更新中,苹果表示该漏洞可能已被用于攻击行为。"这就是我们所说的零日漏洞(0day漏洞),也就是在公司发现并能够做出回应之前,已经被黑客所使用过的漏洞。"美国麦迪安网络安全公司(Mandiant)的高级威胁情报顾问杰米·科利尔(Jamie Collier)说。

在前述360漏洞研究院人士看来,虽然苹果在声明中用了"可能"两字,但结果上和逻辑上已经说明该漏洞被"利用"了,此次苹果不仅修复了这两个漏洞,还针对攻击方法引进了新的防护措施,从而加大了相似漏洞的攻击难度。

安全考验仍在

"在这种情况下依然不断出现在野漏洞攻击事件,对苹果公司来说是重大的考验和挑战。"

张孝荣指出,虽然苹果终端里的系统漏洞相对Windows要少很多,但随着苹果用户的增长,苹果系统日益成为黑客攻击的目标,安全漏洞问题也愈发严重起来。事实上,苹果历史上出现过多次影响重大的漏洞。

"比如2016年的三叉戟漏洞,跟本次修复的漏洞相似,也是通过苹果设备自带的浏览器作为攻击入口,只需要点击恶意链接就可以攻击到内核并接管设备;还有2021年的FORCEDENTRY漏洞,这应该是苹果历史上影响最大的漏洞,因为受害者不需要任何点击,攻击者只需要通过发送iMessage信息到受害者手机上,就可以完成攻击。"前述360漏洞研究院人士说。

有一种观点指出,黑客利用这个漏洞就能在用户不需要点击任何链接的情况下让用户的iPhone中招。对此,前述360漏洞研究院人士指出,黑客想要利用此次漏洞入侵苹果设备还是需要受害者点击链接的,"因为从这次苹果的安全公告来看,苹果修复了这两个漏洞,一是浏览器漏洞,二是内核漏洞,这两个漏洞形成了一个完整的攻击链,受害者只需要点击黑客发送的恶意链接,黑客就能接管苹果设备"。

沦沦认为需要交互。"除非是在同一个局域网,攻击者利用了特定的劫持手段把正常网站比如百度篡改为漏洞EXP,这样用户只要访问了百度就可以直接触发漏洞。"他指出,黑客利用该漏洞的攻击途径包含在局域网内进行扩散,比如同一个WiFi下的ARP(地址解析协议)欺骗植入这种漏洞,或者通过邮件、短信等钓鱼方式让用户点击存在漏洞的链接。

记者注意到,8月17日和18日,苹果中国官方密集发布系统更新,包含iOS 15.6.1、iPadOS 15.6.1、MacOS Monterey 12.5.1、watchOS 8.7.1以及Safari浏览器15.6.1。从更新提示看,以上软件均与安全性有关,苹果也提醒所有用户尽快安装。

前述360漏洞研究院人士指出,该漏洞实际上是新漏洞老手法,攻击方式上没有过于特别的东西,但值得重视的是,近几年苹果公司引入了非常多而且有效的安全防护措施,不断加大攻击难度,在业界也引起了广泛的关注,并且得到广大安全从业者的赞誉,"在这种情况下依然不断出现在野漏洞攻击事件,对苹果公司来说是重大的考验和挑战"。

对普通民众而言,本次漏洞不太可能造成大范围的问题。通常情况下,当iPhone等手机的漏洞被利用时,往往是有针对性的,攻击一般集中于一小部分人。不过,沦沦建议广大用户不要对数字安全和隐私保护放松戒备。

"现在信息泄露这么严重,别人拿到你的信息很容易,如果这个漏洞大范围公开的话,应该会有黑产对信息泄露的一大批人下手,比如批量给他们发短信或邮件信息,诱骗去点击。"因此,他强烈建议广大数字产品用户不要点击来历不明的链接、不要访问一些恶意网站以及公开免费WiFi尽量不要去使用。

用友、金蝶半年报齐现亏损 云服务转型处投入阶段

本报记者 曲忠芳 李正豪 北京报道

近日,国产管理软件两大巨头用友网络(600588.SH)、金蝶国际(00268.HK)分别交出了2022年上半年的成绩单。公告显示,今年1~6月,金蝶国际营收21.97亿元,同比增长17.3%,归属于母公司股东的净亏损为3.56亿元。用友网络今年上半年的营收为35.37亿元,同比增长11.3%,归属于上市公司股东的净亏损为2.56亿元,上年同期净利润为2.15亿元。需要指出的是,不同于金蝶国际连续三年半年报出现亏损,用友网络是近三年里首次出现中期业绩净亏损。

用友网络在公告里表示,同比出现亏损主要是由于去年同期处置畅捷通支付等子公司股权产生的投资收益等的影响,今年同期没有该类收益。归属于上市公司股东的扣非后净亏损为2.06亿元,同比增加了1.25亿元,主要系持续加大研发投入,对业绩释放有一定的滞后性。上半年,用友网络的研发投入为13.17亿元,同比增长38.1%,占营业收入的37.2%。

金蝶国际则在公告中解释称,上半年亏损扩大的主要原因是公司加大了对云服务产品,尤其是金蝶云·星瀚及HR SaaS的研发投入,以及新冠肺炎疫情持续对项目交付效率产生不利影响。

《中国经营报》记者注意到,业界素有"北用友南金蝶"的称呼,分别在北京、深圳创立的这两家公司,均起家于财务软件,后通过ERP(企业资源计划)管理软件成长为国产软件的头部企业,与SAP、甲骨文等国际巨头正面较量,并开启向"云"转型的步伐,几经产品迭代与公司转型改革,在我国软件发展历程中具有典型性和代表性。从用友网络、金蝶国际的2022年中报来看,其云服务业务的增长印证了当前数字化上"云"的大趋势,而亏损的财务状态又表明当前独立软件服务商的云转型仍在持续投入阶段,在数字化转型、信创国产化等趋势红利下,国产软件厂商要实现商业化的跃升仍需要一段时间。

截止到8月24日A股、港股收盘,用友网络的股价报20.69元/股,总市值为710.47亿元;金蝶国际报收14.98港元/股,总市值为520.54亿港元。

近年来,国产软件巨头相继开启了向"云"转型的步伐。 视觉中国/图

云服务业务增长趋势明显

财务数据显示,用友网络、金蝶国际近三年都不同程度地受到了市场环境的影响,经历了2020年上半年新冠肺炎疫情的冲击后,到2021年、2022年上半年已恢复了营收的增长。今年上半年,金蝶国际营收为21.97亿元,同比增长17.3%。其中,76%的收入来自于云服务业务的收入,云服务业务贡献收入16.77亿元,相比上年同期增长了35.5%。而"企业资源管理计划及其他"的收入为5.19亿元,同比则下降了18.1%。具体来看云服务业务的构成——企业云服务收入11.61亿元,同比增长33.69%;小微财务云服务收入3.80亿元,比上年同期的2.18亿元增长74%;行业云服务收入1.36亿元,上年同期为1.51亿元。

云服务业务对总体营收增长的带动作用,在用友网络半年报中也有同样的体现。财报显示,用友网络的营收结构分为"云服务与软件业务"与"金融服务业务"两大部分,今年上半年总体营收35.37亿元中的99%来自于前者,同比增长幅度为19.0%。其中,云服务业务收入22.99亿元,在营收中的贡献占比65.0%,软件业务则继续战略收缩,同比下降16.1%,实现收入12.12亿元。

半年报披露,截止到今年6月末,用友网络云服务累计付费客户数为50.45万家,上半年新增云服务付费客户数为6.62万家。金蝶国际根据不同客户类型披露各产品的客户数,面向大型企业的金蝶云·苍穹、星瀚收入2.84亿元,签约客户累计476家,上半年新增194家,面向中型企业的星空云客户数达2.83万家,而适用于小微企业的小微财务云客户数近2万家。

不难看出,云服务业务已担纲用友网络、金蝶国际的营收及增长主力。这一趋势从其对标的国际巨头SAP(NYSE:SAP)的最新业绩报告中同样得以呈现。今年1~6月,SAP总收入为145.94亿欧元,云和软件业务收入总体贡献125.19亿欧元,其中云业务收入58.76亿欧元,同比增长33%,非国际财务报告准则下云业务的毛利率达到71.0%。截止到第二季度末,SAP的云订单积压金额为104.03亿欧元,同比增长34%。

增收未增利,投入持续加大

尽管云服务业务的增长明显,但今年上半年,用友网络、金蝶国际的半年业绩却均出现净亏损的局面。今年上半年,用友网络归属于上市公司股东的扣非后净亏损2.06亿元,公告中指出,主要是因为持续加大研发投入,落实"强产品"关键任务,增强云服务产品的平台、核心应用和生态融合能力。数据显示,该公司上半年研发投入为13.17亿元,同比增长38.1%,占营收的37.2%。

金蝶国际在2020~2022年这三年的半年业绩中,归属于母公司股东的净亏损额度不断扩大,分别为2.24亿元、2.48亿元、3.56亿元。今年上半年,金蝶国际围绕"平台+人财税+生态",加大了对金蝶云·苍穹、星瀚的投入力度,研发成本总额为7.95亿元,同比增长19.0%。

本报记者注意到,用友网络、金蝶国际均成立上世纪90年代前后,从财务软件发展到ERP管理服务,而在2015年前后向"云"转型。2014年,金蝶国际创始人、董事会主席兼CEO徐少春在发布会上抡起大锤砸掉传统服务器,至今被业界津津乐道;2016年,用友网络董事长、总裁王文京提出用友实施以"企业互联网服务"为主体业务的3.0战略,向云服务转型。无论是金蝶国际,还是用友网络,在向云转型的过程中并非一帆风顺,金蝶国际"烧钱"抢市场仍在继续,而用友网络经历市值缩水后,2021年,辞去总裁职务两年之久的王文京重新出山,对用友网络"动刀"改革,剥离分拆业务推动子公司IPO。

艾媒咨询高级分析师王清霖指出,用友网络、金蝶国际等软件服务商在今年上半年出现亏损并不意外。自2021年开始,港股、中概股等二级市场整体表现不佳,在这种经济形势下,企业可获得的投资和资金流入较少。而从管理软件行业看,近几年综合类企业管理软件和垂直财务类软件的入局者都明显增加,在这种"僧多粥少"的情况下,管理软件企业的竞争愈发激烈。从企业自身支出看,用友网络、金蝶国际等企业转型和云产品研发投入较大,在营收较少而投入较大的情况下,近几年亏损持续扩大。目前,从企业支出看,大中小型企业都面临着一定的经营压力,大企业的经费缩减、中小企业客户利润低等问题,都令企业的营收面临一定的挑战与压力。

就业绩等相关问题,记者联系采访用友网络和金蝶国际方面,前者暂未回应,金蝶国际则表示以公告为准。

未来增长动力在哪里?

对于未来发展方向及走势,徐少春表示,国产化替代浪潮一浪高过一浪,金蝶国际有能力、也有信心完全替代高端的国外管理软件。公司在大企业市场已经取得一些成绩,有信心用两到三年时间夺取市场份额,对于中小企业市场,公司将继续稳固地盘、扩大优势。

金蝶国际在今年上半年拓展新客户的同时,用友网络在半年报中也提到了信创产业增长的机会,国家持续加大对科技创新的支持力度,信创产业上升至国家战略,将以新一代技术和产品进行企业数智化的升级换代为背景和基础,形成数智化升级+信创的价值。用友网络援引《2022中国信创生态市场研究及选型评估报告》数据称,2022年信创产业规模达9220.2亿元,预计2025年将突破2万亿元,五年复合增长率将达36%。

根据前瞻产业研究等第三方机构的研究报告,国内ERP市场已由用友网络、金蝶国际、浪潮软件、神州数据等本土厂商占据主要份额,本土品牌的崛起已成为中国ERP市场的主要发展趋势。不过,高端ERP软件市场,SAP、甲骨文等国外厂商则拥有较为稳固的份额。

王清霖解释道,ERP企业资源计划软件,是基于信息技术为企业管理层和员工提供信息化决策的系统管理平台。随着企业需求的发展,ERP系统已经从单纯的财务管理发展为企业管理中的更多需求,这也是目前部分ERP系统被称为"高端ERP"的主要原因。国外厂商的ERP系统业务发展较早,具有一定的技术优势。但是单从技术本身看,国内企业与国外的差距不大。更关键的是,海外SAP、Oracle等企业的企业文化与国外的世界500强企业更加契合,同时,这些企业具有一段时间的服务海外企业经验,具有更多的数据资源和服务基础,因此,在全球市场地位较为稳固。而得益于中国数字经济的迅猛发展,中国信创市场释放出前所未有的活力,并且在国家大力支持自主研发的政策背景下,企业特别是这类高端管理企业软件的国产化,可以更好地获得政策支持和客户买单。不过,除了政策支持、风口效应等市场"红利"之外,要想长期留住企业客户、获得投资及市场的认可,国产软件仍需要持续强化自己的产品,为大企业和中小企业分别推出不同的定制策略,同时通过出海寻求增量市场,形成增长的新动力。