白豚
WhiteDolphin

可靠性说明

白豚
WhiteDolphin

概述

- 白豚 ERP 系统通过在线复制（分布式文件系统）、磁盘快照、自动备份和自动恢复、数据强加密、CHAP 鉴权、TLS（HTTPS） 安全传输、以及高可用集群（HAC）等多种手段，从数据存储、网络传输、节点容错等各个方面来保证 ERP 服务的安全性、可靠性、稳定性和健壮性。

白豚
WhiteDolphin

数据可靠性

- 跨 IDC 的分布式 6 副本技术，确保包括业务数据、配置数据、附件数据在内的所有 ERP 数据可靠性均高达 17个9（99.99999999999999%）。即使整座 IDC 被灾难性地完全摧毁，也不会丢失任何数据。

- 云平台每日自动完成快照备份，保留最近 7 天和 90 天内每周末的磁盘快照（7+12）。快照数据基于可靠的双重EC算法，可有效找回由员工误操作或恶意操作引起的数据丢失。备份快照交错储存于不同的 IDC 机房中，以进一步提升其可靠性。

- 配置数据集中存放在由我方自主研发的，带有实时（on-the-fly）压缩和强加密保护的虚拟文件系统（VFS）中。每次配置变更时，都会对配置数据进行自动备份。每次数据访问前，都会对配置数据进行完整性检查，若发生错误，则对其进行自动恢复。

白豚
WhiteDolphin

服务可用性

- 由我方自主研发，基于多数派算法的强一致抗脑裂（Split Brain）多活 IDC 高可用集群（HAC）专利架构，服务整体可用性可达 6个9（99.9999%）。确保即使整座 IDC 由于市政施工、自然灾害、人为失误等原因下线，也可在秒级完成故障转移，自动切换到其它可用 IDC 不间断提供服务。

- 精心设计的故障检测、服务发现、服务选举、分布式锁以及消息路由等分布式协调和数据同步算法提供的强一致性保证确保了跨 IDC 的故障转移也不会导致数据一致性问题。

注：我方高可用（HAC）、高性能（HPC）分布式架构和算法受到多项国家和国际发明专利保护。

白豚
WhiteDolphin

可靠性补充说明

- 带强一致保证的多活 IDC 技术是现代高性能和高可用集群的关键技术，也是业界公认的主要难点。作为实例：2018 年 9 月 4 日微软美国中南区某数据中心空调故障导致 Office、Active Directory、Visual Studio 等服务下线近 10 小时不可用； 2015 年 8 月 20 日 Google GCE 服务中断 12 小时并永久丢失数据；2015 年 5 月 27 日和 2016 年 7 月 22 日支付宝两次中断数小时；以及 2013 年 7 月 22 日、2023 年 3 月 29 日微信服务中断数小时等重大事故均属于产品未实现多活 IDC 架构，单个 IDC 故障导致服务全面下线的惨痛案例。
- 在上述方面，我方拥有超过十年的丰富积累，受多项国家和国际发明专利保护的分布式架构和算法。得益于领先的强一致、高可用、高性能分布式集群算法和架构，我们在白豚 ERP 平台上实现了真正的强一致多活 IDC 架构，为客户提供了无以伦比的数据可靠性和服务可用性保证。

白豚
WhiteDolphin

可靠性补充说明 - 微信未实现多活 IDC, 导致瘫痪数小时

微信全面瘫痪：服务器故障 国内外均无法连接

中国网 www.china.com.cn 2013-07-22 10:02 打印 | 转发 | 评论

中国网7月22日讯(记者 乔红康)7月22日早间，有大量用户反映腾讯微信发生故障，包括微信信息无法发出、无法刷新朋友圈、无法登陆公众账号平台、无法连接微信网页版等。

从网友反馈的结果来看，包括北京、广东、浙江、山东、黑龙江、河南等地区在内，微信均发生全面故障。有用户表示，目前他人在美国，但也连不上微信。

腾讯微信官方微博对此发布回应称，由于服务器基础网络故障导致出现收发问题，并表示正在恢复中。截至22日上午10:00整，该故障仍未修复。

近期，微信多次出现相关故障，仅在上个月就连续出现多次登录、公众平台、连接服务器等方面的故障。

白豚 WhiteDolphin

可靠性补充说明 - 微信QQ未实现多活 IDC, 导致瘫痪数小时

RSS订阅

中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

工业和信息化部 新闻动态 政务公开 政务服务

首页 > 工业和信息化部 > 机关司局 > 信息通信管理局 > 应急通信与互联互通

工业和信息化部信息通信管理局指导重要业务系统安全稳定运行

间：2023-04-14 16:57 来源：信息通信管理

局听取腾讯公司关于“3·29”微信业务异常情况汇报，要求腾讯公司进一步健全安
坚决避免发生重大安全生产事故，切实提升公众业务安全稳定运行水平。
局将深入贯彻落实党的二十大报告关于提高公共安全治理水平的决策部署，统筹发展
管力度，指导电信业务经营者严格落实主体责任、完善保障措施、强化事故应急处置
行业高质量发展。

工信部听取“3•29”微信业务异常情况汇报，腾讯：已处罚相关负责人

红星新闻 2023-04-14 21:28

红星资本局4月14日消息，据工信部官网，工信部信息通信管理局听取腾讯公司关于“3·29”微信业务异常情况汇报，要求腾讯公司进一步健全安全生产管理制度、落实网络运行保障措施，坚决避免发生重大安全生产事故，切实提升公众业务安全稳定运行水平。

对此，腾讯方面的相关负责人向红星资本局表示，3月29日凌晨，由于机房配套设施故障，部分用户使用微信相关功能时出现异常。事故发生后，微信内部快速拉起了专项团队，对问题予以解决，并进行全链条梳理、优化产品保障机制。

腾讯微信团队
3-29 10:50
工程师淋汗以报：现在微信、微信支付相关功能已恢复。

@腾讯微信团队
今天凌晨部分用户使用微信、微信支付相关功能出现异常，经工程师抢修，系统正在逐步恢复，很抱歉给大家带来不便。
3-29 08:44 1079 6604 1.8万

96 2215 1332

腾讯微信团队
3-29 08:44
今天凌晨部分用户使用微信、微信支付相关功能出现异常，经工程师抢修，系统正在逐步恢复，很抱歉给大家带来不便。
1079 6604 1.8万

白豚 WhiteDolphin

可靠性补充说明 - 支付宝未实现多活 IDC, 导致多次瘫痪数小时

可靠性补充说明 - 谷歌云计算服务瘫痪 12 小时并永久丢失数据

谷歌数据中心遭雷劈 部分数据永久丢失

腾讯科技 [微博] 2015年08月20日18:19 我要分享

[摘要]雷电天气引起电力中断，导致数据中心磁盘受损和云存储系统断线。

腾讯科技讯 8月20日，比利时布鲁塞尔西南郊的St.Ghislaina小镇日前遭遇了强雷电天气，而这一恶劣天气的出现也让谷歌(微博)位于当地的数据中心不幸“躺枪”。

谷歌方面表示，当时的雷电天气引起了电力中断，导致磁盘受损、部分云存储系统断线、数据丢失。虽然数据中心很快便切换到了备用电源，但这一切换却依旧导致0.000001%的数据遭到了删除，且无法恢复。

对此，一家名为“Azendoo”的法国初创企业负责人查尔斯-大卫(Charles David)表示，因为谷歌数据中心遭遇雷击，自己公司的服务遭遇了长达12小时的中断。

在随后发布的官方事故报告中，谷歌表示自己需要为这一事件负上全部责任，同时鼓励受到影响的企业用户考虑将数据备份到其他谷歌存储服务中。

“谷歌云计算引擎的此次事故表明，企业将所有数据存储在单一数据中心会不可避免的在遭遇数据中心级别意外时候面临巨大风险。”谷歌在自己的官方声明中说道。

对于谷歌的这一说法，Proper Villains公司合伙人阿隆-图比克（Aaron Trubic）也非常赞同。

白豚 WhiteDolphin

可靠性补充说明 - QQ 邮箱未实现多活 IDC, 服务大规模瘫痪

就 QQ邮箱等产品大规模瘫痪 作出说明

发布时间：2015-03-20　更新时间：2015-03-31　来源：网络　作者：natty

关键词： 腾讯 公告 网络故障

技术资料　云计算　云服务器ECS　rds　大数据　建站　com域名　软件安装　域名注册

1月21日中午消息，腾讯客服今日发布公告，就 QQ邮箱等产品大规模瘫痪 作出说明。公告指出，由于网络系统故障，QQ空间、QQ邮箱等16款腾讯旗下产品受到影响，目前相关服务正在恢复中。

今日早些时候有消息指出，本次QQ邮箱无法正常登陆的原因是，腾讯第三方登录服务器出现了宕机，但腾讯官方未就此作出回应。

今天上午，多家媒体及微博大号报道了腾讯多款产品无法正常使用的情况，不少网友调侃称 “腾讯出事了，出大事了，年终奖发少了，技术把服务器格式化了！”

截至记者发稿，此次网络故障所影响的产品已经基本恢复正常。(木南)

腾讯公告原文：

关于网络故障造成部分业务无法正常使用的通知

尊敬的用户：

您好，非常抱歉，由于网络系统故障，导致您的部分服务使用可能受到影响，目前相关服务正在恢复中，请您稍后再使用，由此给您带来的不便敬请谅解！感谢您的支持。

白豚 WhiteDolphin

可靠性补充说明 - 阿里云机房多次故障导致服务中断

尊敬的阿里云用户：

您好，杭州可用区D网络故障确认由于市政施工导致运营商光纤受损 ，现场正在紧急抢修，目前部分链路已经恢复，请您协助我们一起测试观察，详细情况我们稍后给

给您带

阿里云计

2014年1

3月3日凌晨，阿里云开始出现大规模故障，位于华北地区的多家互联网公司的 IT 运维人员发现
后一批程序员赶往公司加班。这起宕机事故持续了三个小时左右，事后观察了两个小时。

阿里云

公告

阿里云首页 > 其他 > 【其它】关于华北2地域可用区C部分EC

【其它】关于华北2地域可用区C部分ECS服务器IO HANG通报

北京时间2019年3月3日凌晨，华北2地域可用区C部分ECS服务器等实例出现IO HANG，经紧急排查处理后已全部恢复。目前我们已经全面排查其他地域及可用区，未发现此类情况。

非常抱歉给您带来的影响！如有任何问题，可通过电话工单随时反馈，感谢您的理解和支持！

针对本次故障，我们将根据SLA协议，尽快处理赔偿事宜。

阿里云计算有限公司
2019年3月3日

阿里云官方公告

阿里云香港机房为何瘫痪12小时

2015年06月23日 20:53 来源于 财新网

事故发生24小时后，阿里云和运营商对事故原因和细节仍莫衷一是，甚至无辜的消防和电力部门也被拉来躺枪。阿里云作为国内最大的互联网云提供商是否已经准备好

相关报道

【财新周刊】以阿里云击IOE

【大家谈】阿里云：冲着第一而来

阿里云海外扩张提速 借迪拜拉进中东北非

中石化牵手阿里云 开启能源大数据

12306春运火车票查询75%由阿里云分流

中国驰虎邮箱将关 阿里云接管

阿里蚂蚁金服60亿建本地生活O2O平台

阿里CEO张勇：做生意的方式将深刻改变

歌华联手阿里、中影打造中国电视院线（更新）

阿里挑战CDN玩法

阿里当家 网商银行能飞多高

【财新网】（记者 屈运祖 驻香港记者 王婧 见习记者 刘晓景）没有挖断光纤，也不是电力部门问题，更没有所谓的消防警报延误抢修时间。经过财新记者多方调查核实，阿里云在香港中止服务12小时就是一起由硬件故障引发、抢修和恢复严重超时的事故。

这类数据中心的电力事故原本是国内外云服务商普遍面临的一大问题，但用一位业内资深人士的话来说，“12小时才恢复实在太久了。应该几分钟就解决的。”

12小时的超长处理时间，以及过程当中阿里云与相关方陆续给出的五花八门甚至自相矛盾的解释引发了用户的不满和业内的质疑，也暴露了阿里云在故障处理和公众沟通中存在的问题。有部分用户甚至反映15个小时业务才恢复。

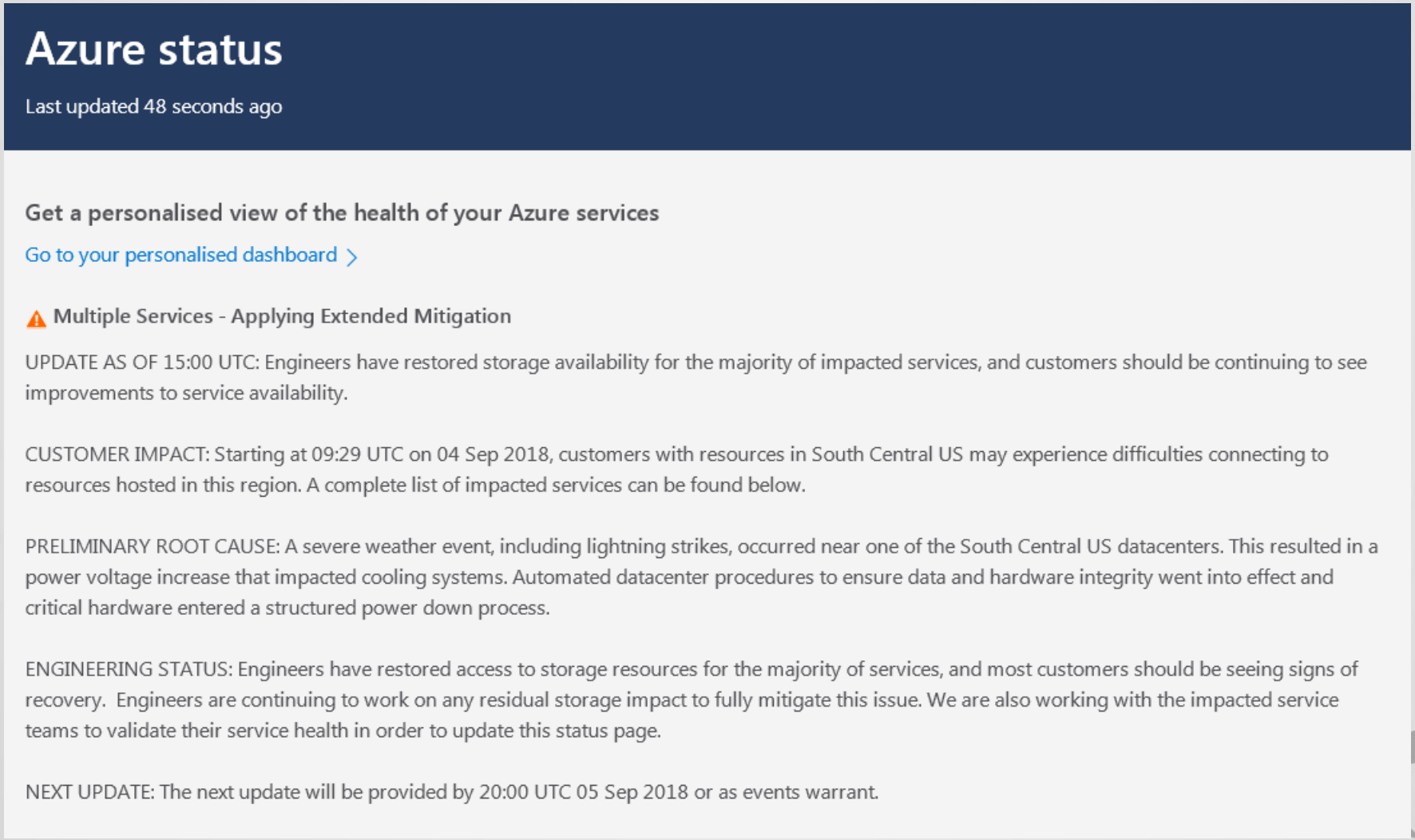
白豚 WhiteDolphin

可靠性补充说明 - 英国航空因机房电力故障导致系统瘫痪数日

白豚
WhiteDolphin

可靠性补充说明 - 微软机房故障导致不可用

- 微软某机房空调故障导致 Office、AD、VS 等服务下线近 10 小时不可用



Azure status

Last updated 48 seconds ago

Get a personalised view of the health of your Azure services

Go to your personalised dashboard >

⚠ Multiple Services - Applying Extended Mitigation

UPDATE AS OF 15:00 UTC: Engineers have restored storage availability for the majority of impacted services, and customers should be continuing to see improvements to service availability.

CUSTOMER IMPACT: Starting at 09:29 UTC on 04 Sep 2018, customers with resources in South Central US may experience difficulties connecting to resources hosted in this region. A complete list of impacted services can be found below.

PRELIMINARY ROOT CAUSE: A severe weather event, including lightning strikes, occurred near one of the South Central US datacenters. This resulted in a power voltage increase that impacted cooling systems. Automated datacenter procedures to ensure data and hardware integrity went into effect and critical hardware entered a structured power down process.

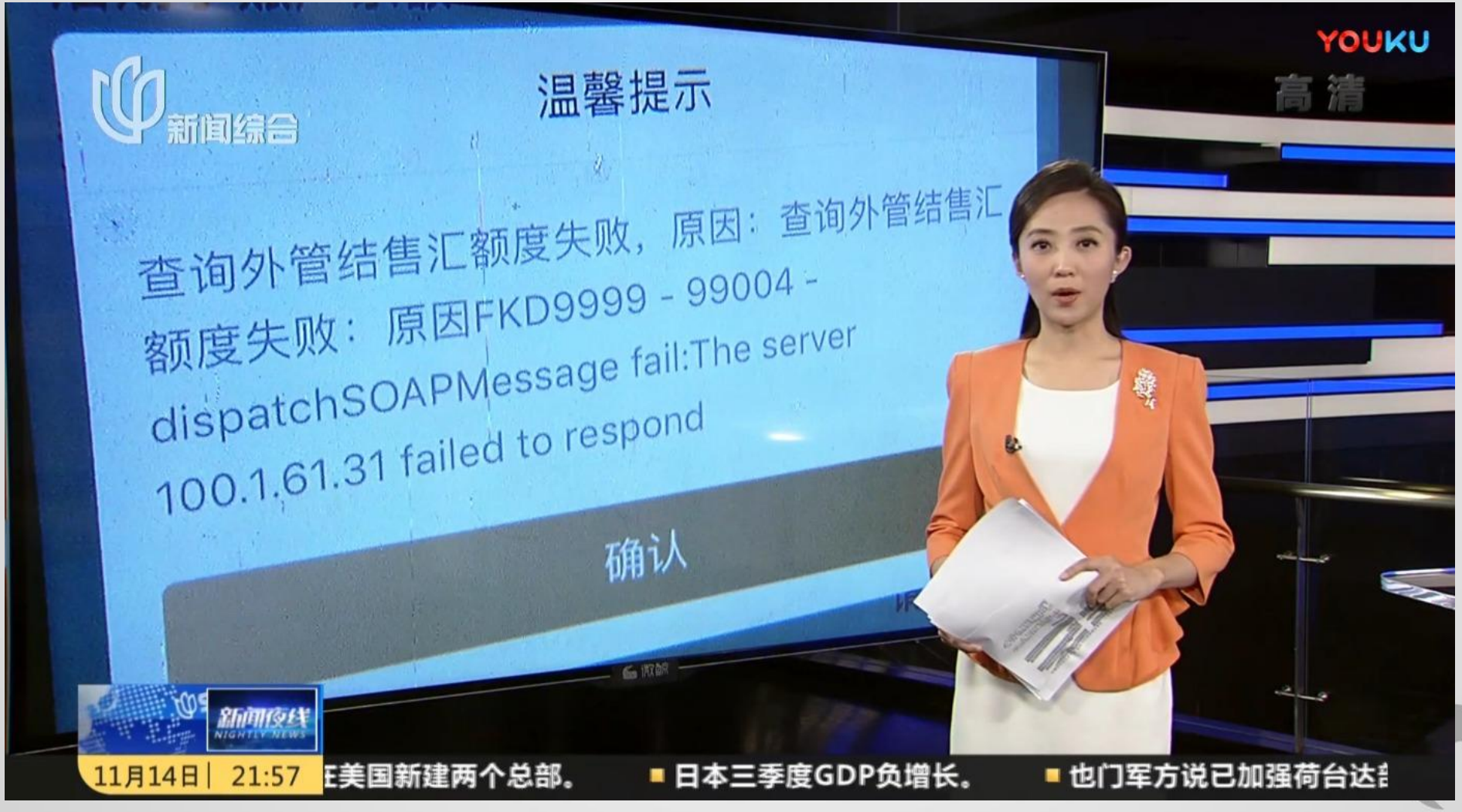
ENGINEERING STATUS: Engineers have restored access to storage resources for the majority of services, and most customers should be seeing signs of recovery. Engineers are continuing to work on any residual storage impact to fully mitigate this issue. We are also working with the impacted service teams to validate their service health in order to update this status page.

NEXT UPDATE: The next update will be provided by 20:00 UTC 05 Sep 2018 or as events warrant.

白豚 WhiteDolphin

可靠性补充说明 - 国家外汇系统故障导致不可用

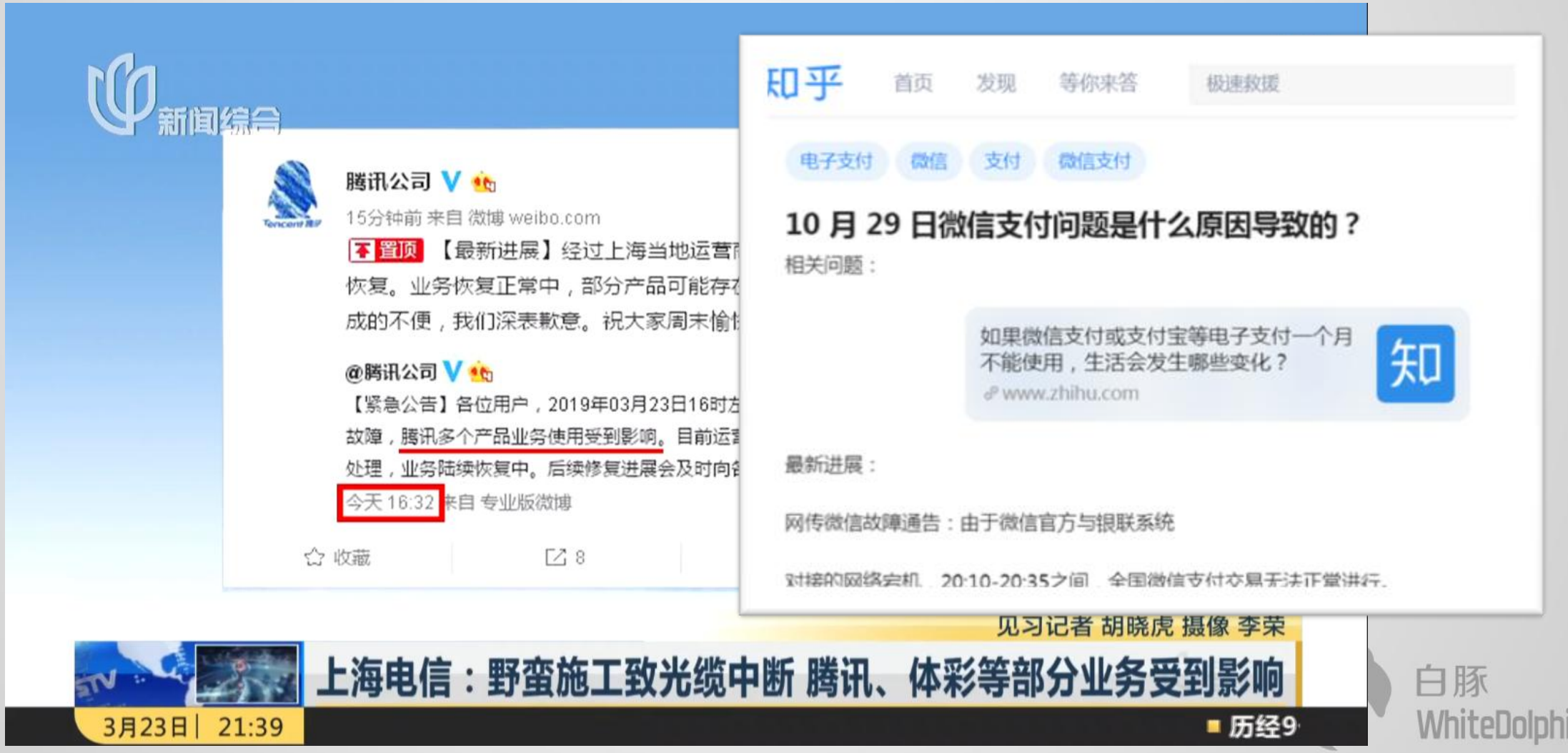
- 国家外汇系统发生故障导致国内所有银行外汇兑换业务停止数小时



白豚
WhiteDolphin

可靠性补充说明 - 电信光纤断开导致腾讯多项业务不可用

- 上海电信光纤被挖断导致腾讯英雄联盟（LoL）等多项业务停止数小时



白豚 WhiteDolphin

数据安全性 - 1

- 白豚 ERP 使用基于我方自主研发，支持实时（on-the-fly）数据压缩和强加密的虚拟文件系统（VFS），对数据库，和所有配置信息提供整库级别的强加密保护，支持包括 AES、BlowFish、SERPENT 在内的数十种业界认可的强加密算法。

注：普通的，以数据库记录为单位的加密通常会将相同的明文转换为同样的密文。

例如：若数据库内的用户表中，有一个名为 Name 的字段用来存放员工姓名，并且明文“张三”被加密后的密文为 “ABCD”，则对于逐行（逐字段）加密的算法来说，表中每次出现名为“张三”的员工，都将被加密为“ABCD”（类 ECB 模式）。

所有类 ECB 模式对静态分析、差分分析、已知部分明文攻击等破解手段防护能力都很弱，无法确保数据安全。

白豚 ERP 使用基于 CTR 模式和 AES 等强加密算法的整库加密技术，提供数学上可证明的强安全性（可靠性、一致性、保密性）保护。即使是相同的明文，也会被变换为不同且完全无关的密文，从而杜绝了上述攻击方式。

白豚
WhiteDolphin

数据安全性 - 2

- 白豚 ERP 使用加盐的安全散列值存储用户密码。这些信息将经过压缩和强加密处理后才保存到配置存储中。

- 白豚 ERP 使用基于角色的严格授权机制和访问控制列表（ACL）统一管理用户权限。在开启了整库加密功能后，即使网络管理员也无法窥视企业数据。

白豚
WhiteDolphin

传输安全性

- 白豚 ERP 使用公认权威机构发布的数字证书，提供网银级别的 TLS（HTTPS）网络数据传输保护。

- 用户密码以加盐安全散列的形式进行存储。使用基于 SHA 和 HMAC 安全算法的 CHAP 鉴权协议完成网络鉴权流程。即使不依赖 TLS 加密保护（全明文传输），也不会发生密钥泄露。

- 同一用户连续 5 次登陆失败后，强制冷却 5 分钟，配合入侵检测和恶意请求过滤技术，防止暴力破解。此外，管理员还可自定义最小长度，大小写字母和数字组合等密码复杂度要求。

白豚
WhiteDolphin

系统安全性 - 1

- Java（JRE）、C#（.NET）以及 Tomcat 等环境存在大量严重漏洞，有极高安全隐患。通过国际安全组织公开的 CVE 数据库可发现，上述产品几乎每年都会产生多个安全等级为“严重”的新漏洞。例如：

- Java：https://www.cvedetails.com/vulnerability-list/vendor_id-93/product_id-19117/Oracle-JRE.html

- Tomcat：https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-887/Apache-Tomcat.html

- .NET：https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-2002/Microsoft-.net-Framework.html

- 等等。

白豚
WhiteDolphin

系统安全性 - 2

- 如左图所示：对 Java、.NET 等动态运行时环境、Tomcat 等容器，以及 JBoss 等第三方框架的依赖，导致系统中被引入了大量额外的，不受开发商控制的第三方组件。

- 可以看到，使用 Java、.NET、PHP 等动态语言开发的产品，其应用程序与底层基础设施间包含了第三方框架、Web容器、动态运行时等多个额外层面。这些不受开发商控制的，由第三方软件组成的额外层面包含大量广为人知，可被轻易利用的安全漏洞。

白豚 WhiteDolphin

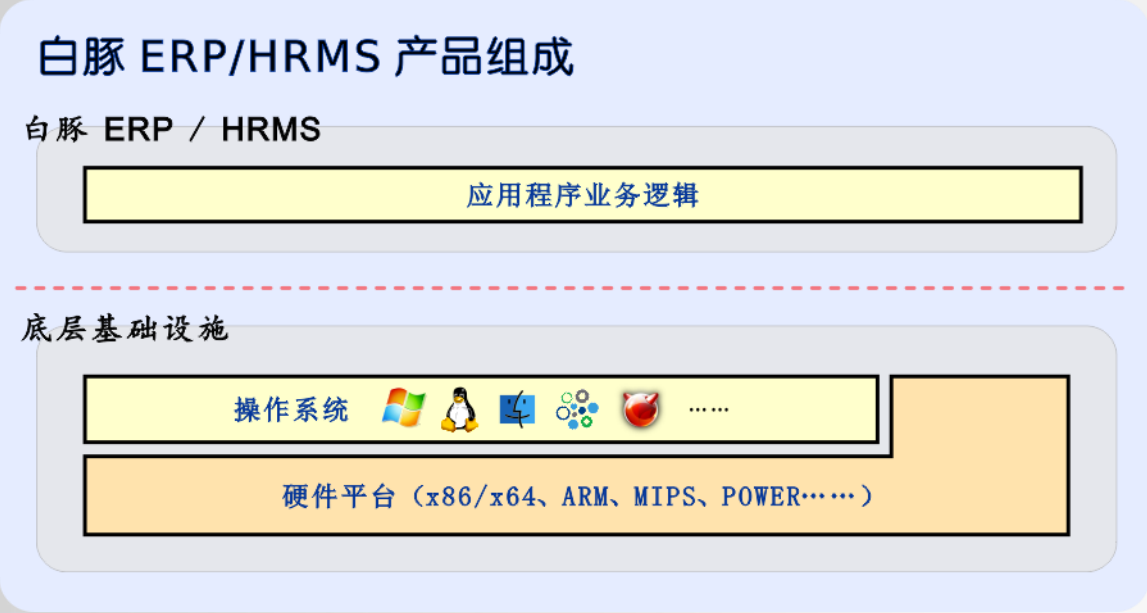
系统安全性 - 3

- 甚至任何稍有常识的普通用户都可以通过搜索引擎简单地找到可成功利用这些漏洞进行攻击的免费开源工具，并以此入侵企业系统，完成数据窃取、数据篡改、数据销毁等非法操作。

- 由此可见，引入不受控制的额外层面大大增加了系统的受攻击面，严重增加了系统的安全风险。同时大大增加了运维人员的工作负担，提升了系统的总体拥有成本（CTO）。

白豚
WhiteDolphin

系统安全性 - 4



- 如上图所示：白豚 ERP/HRMS 系统使用汇编、C/C++等工具开发。
- 直接构建在底层操作系统和硬件平台之上。

- 白豚以高效的原生机器码（ Native Code ）直接运行在裸硬件和操作系统构成的底层基础设施上，为 ERP 系统带来了无与伦比的时空效率和安全性保障。

- 由于无需依赖动态运行时、Web容器等不可控的第三方组件，因此大大减少了软件的受攻击面，极大地降低了系统安全隐患。同时在很大程度上减轻了运维人员的工作负担，降低了客户总体成本。

白豚
WhiteDolphin

安全性补充说明 - 1

- 近年来安全问题频发，亚马逊、沃尔玛、Yahoo、Linkedin（领英）、索尼、摩根大通、UPS、eBay、京东、支付宝、协程、12306、网易、CSDN、中国人寿、以及各大酒店集团（锦江、洲际、喜来登、万豪等）等国内外知名企业均频频报出大量用户信息泄露的严重安全事件，安全保障已经刻不容缓。

- 白豚所有数据库（整库）和本地配置数据均存放在我方自主研发的，支持实时（on-the-fly）数据压缩和强加密的虚拟文件系统（VFS）中，进行全方位保护，支持数十种业界公认的强加密安全算法，即使系统管理员也无法窥视企业数据。

- 基于业界标准的强加密算法保证了即使未来出现了每秒钟可完成一千万亿次密钥破解尝试的超级计算机，也需要平均五千四百万亿年才能破解一个密钥。安全性得到了极大保证。

白豚
WhiteDolphin

安全性补充说明 - 2

思科：Java 成 91% 恶意攻击的主要原因

oschina 发布于2014年03月18日 收藏 15 评论 21

Google、Github 双重认证前端课程，独家硅谷内容，每周直播辅导，限时报名>>> HOT

思科的2014年度安全报告中指出：甲骨文公司的Java技术成为安全问题的主要来源。

根据思科最近的安全报告，在2013年，IT企业面对着各种各样的网络攻击和风险。但是，没有任何一项技术会遭到如此多的吐槽，除了Java。

思科的2014年度安全报告发现，Java占据了2013年所有安全问题91%的比例。

“在观测到的网络攻击中，Java贡献了大份额的负载值。”来自思科技术部门的技术主管莱维·贡德特向eWEEK（译注：美国互联网媒体）透露。

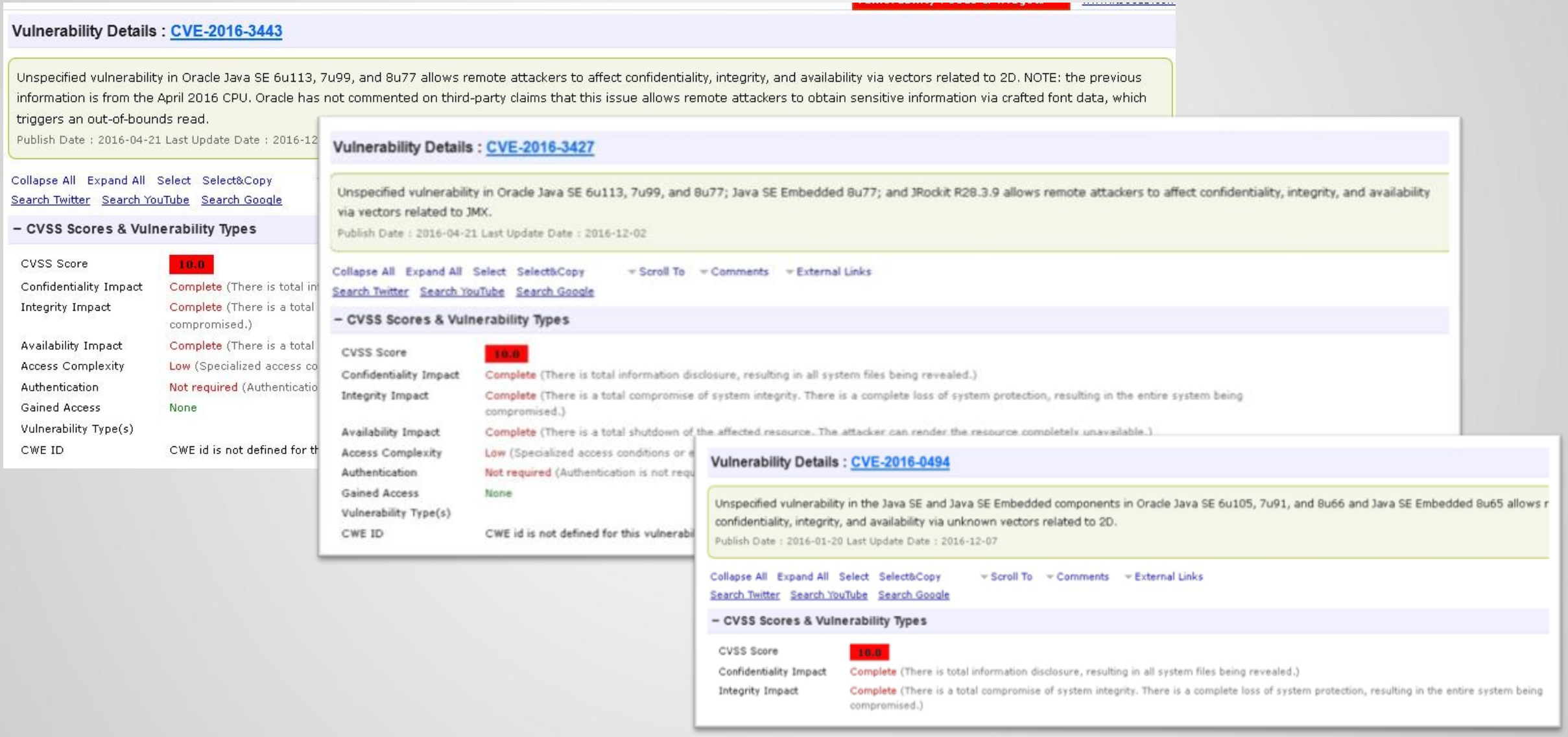
思科的安全威胁研究部门在安全威胁报告中披露了Java的相关数据，该部门在2013年被思科以27亿美元收购。

贡德特说道：“我惊讶地发现，Java引发的网络安全攻击占据了91%的比例！其中有一些攻击是利用了Java的‘零时差攻击’（零时差攻击，即安全补丁与瑕疵曝光的同一日内，相关的恶意程序就出现并对漏洞进行攻击的一种形式）漏洞。当然，也有很大一部分则是利用了我们已经知道的Java漏洞。”

思科不是唯一一家发现Java攻击数量在2013年上升的企业。包括惠普和卡巴斯基实验室在内的公司也发现Java攻击在2013年激增。1月15日甲骨文再次推送Java更新，这次更新覆盖了51个漏洞。

白豚 WhiteDolphin

安全性补充说明 - 3: Java 高危漏洞一瞥



Vulnerability Details : CVE-2016-3443

Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to 2D. NOTE: the previous information is from the April 2016 CPU. Oracle has not commented on third-party claims that this issue allows remote attackers to obtain sensitive information via crafted font data, which triggers an out-of-bounds read.

Publish Date : 2016-04-21 Last Update Date : 2016-12

Collapse All Expand All Select Select&Copy
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total in
Integrity Impact	Complete (There is a total compromised.)
Availability Impact	Complete (There is a total
Access Complexity	Low (Specialized access co
Authentication	Not required (Authenticatio
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for th

Vulnerability Details : CVE-2016-3427

Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX.

Publish Date : 2016-04-21 Last Update Date : 2016-12-02

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or
Authentication	Not required (Authentication is not requ
Gained Access	None
Vulnerability Type(s)	
CWE ID	CWE id is not defined for this vulnerabi

Vulnerability Details : CVE-2016-0494

Unspecified vulnerability in the Java SE and Java SE Embedded components in Oracle Java SE 6u105, 7u91, and 8u66 and Java SE Embedded 8u65 allows r confidentiality, integrity, and availability via unknown vectors related to 2D.

Publish Date : 2016-01-20 Last Update Date : 2016-12-07

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)

安全性补充说明 - 4: 安全漏洞导致 Yahoo 泄露超 30 亿用户数据

雅虎再次曝出数据泄露事件：涉10亿帐户 有史以来最严重

2016年12月15日 09:07 新浪科技 微博

雅虎：5亿用户信息两年前被盗 或为最大网络信息泄露 东方新闻 160923

雅虎又泄露3200万账户数据，这次是因为“cookie伪造”攻击

孙毛毛 2017-03-03 共39169人围观，发现 18 个不明物体 资讯

前科技巨头雅虎近期公布的消息显示：在过去两年间，有入侵者进行“cookie伪造”攻击，造成3200万账户泄露。特别要说明的是，此次泄露事件是独立存在的，和前几个月爆出的两次大规模数据泄露不一样（2016年12月曝10亿账户泄露，9月曝5亿账户泄露）。当然，3200万这个数字现在听起来根本就不算什么。

engadget 中国版

雅虎承认 2013 年的骇客攻击涉及了当时所有 30 亿个账户

受害者数量一下子变成了之前公布的三倍。

Sanji Feng
2017 年 10 月 4 日, 下午 08:00

盗 或为最大网络信息泄漏 NEWS24

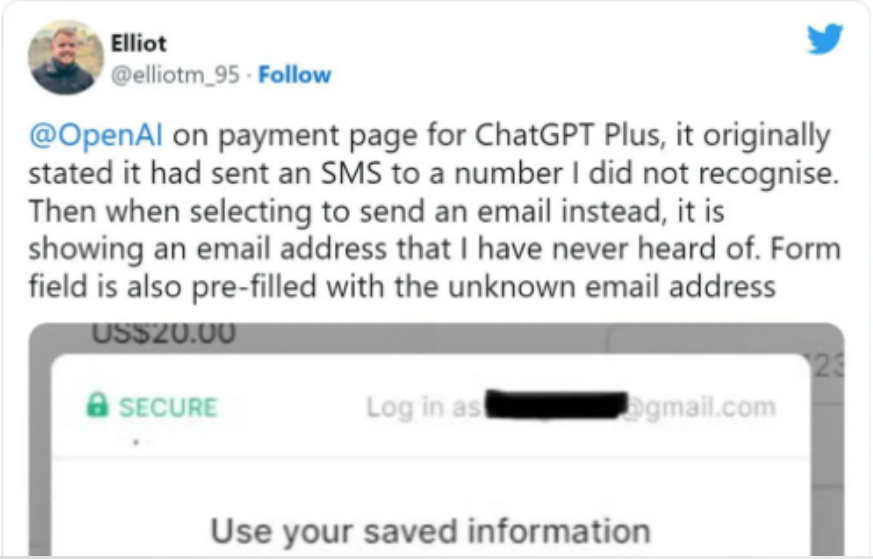
WhiteDolphin

安全性补充说明 - 5: Redis 安全漏洞导致 ChatGPT 隐私数据泄露

Redis 错误导致 ChatGPT 数据泄露，技术细节一并公布

来源: OSCHINA 编辑: Alias_Travis 2023-03-27 08:52:26 8

在上周一，ChatGPT 遭遇了一次用户数据泄漏事件，许多 ChatGPT 的用户都在自己的历史对话中看到了其他人的对话记录。不光是对话的历史记录，不少 ChatGPT Plus 用户还在 Reddit 和 Twitter 等平台发出了截图，表示在他们的订阅页面上看到了其他人的电子邮件地址。



白豚 WhiteDolphin

安全性补充说明 - 6: 网易泄露过亿用户数据

网易邮箱被曝过亿数据泄露

腾讯科技 [微博] 梁辰 2015年10月19日15:39 我要分享

腾讯科技讯（梁辰）10月19日，有用户“路人甲”在国内安全网络反馈平台WooYun（乌云）发布消息称，网易163/126邮箱过亿数据泄漏，涉及邮箱账号、密码、用户密保等。这一漏洞危害等级被标注为“高”。另有消息称，此次泄露规模或达5亿条的规模。同时也有人表示，已向苹果客服咨询，苹果客服称网易服务器被入侵。

不过，截至腾讯科技发稿时，乌云平台已将“网易邮箱”抹掉，改为“某邮箱”。目前的漏洞状态为已交由第三方合作机构(cncert国家互联网应急中心)处理。

导致此次安全事件的原因，疑似网易用户数据库泄露，影响数量总共数亿条。乌云方面称，目前已通过乌云漏洞平台第一时间通知到网易。

乌云平台披露，目前泄露的信息包括用户注名、MD5（一种算法）密码、密码提示问题和答案、注册IP、生日等。据悉，解开后测试大部分邮箱依旧还可登陆。

白豚 WhiteDolphin

安全性补充说明 - 7: Java Struts 框架漏洞致京东数千万用户泄露

白豚
WhiteDolphin

安全性补充说明 - 8: 支付宝泄露数千万用户数据

支付宝数据泄露!工信部介入密码泄露调查

字号 大 小

2011年12月30日11:06 来源： 太平洋电脑网 作者：盛夏Veya 欢迎发表评论

将本文转发至： 纠错 | 收藏

12月30日消息，中国互联网正在遭遇一场最大规模的用户信息泄露事件，而此次“泄密门”事件波及的范围也越来越广，从互联网科技公司，到互联网电商企业，都难逃数据泄露的厄运。而如今，就连银行、出入境局登记数据也被传有泄露。目前，工信部已经介入此次大规模的密码泄露事件，强烈谴责窃取和泄露用户信息的行为，责令发生用户信息泄露的网站尽快发出警示，要求互联网站开展全面的安全自查。

不断扩大的互联网用户信息泄露阴影

继CSDN、天涯社区等论坛确认用户资料被泄露之后，一向被用户定义为“安全”的第三方支付平台也被爆料称上千万的用户信息外泄。

漏洞概要 关注数(8)

缺陷编号： WooYun-2011-03871
漏洞标题： 支付宝用户大量泄漏，被用于网络营销
相关厂商： 支付宝
漏洞作者： 路人甲
提交时间： 2011-12-28
漏洞类型： 用户资料大量泄漏
危害等级： 高
自评Rank： 20
漏洞状态： 等待厂商处理
漏洞来源： http://www.wooyun.org
Tags标签： 无
分享漏洞：

漏洞详情

简要描述：

支付宝用户大量泄漏，被用于网络营销 泄漏总量达1500-2500W之多 泄漏时间不明，里面只有支付宝用户的账号，没有密码

漏洞hash：6701ae23372bbea6c1dd74f23d8c584e

支付宝用户信息也被泄露

日前，网络安全问题反馈平台“乌云漏洞”指出，支付宝部分账号信息被泄露，涉及邮箱数量在1500万至2500万。对此，支付宝公关经理朱先生否认支付宝存在漏洞一说，并称相关账号并

白豚 WhiteDolphin

- 安全性补充说明 - 9: 信用巨头 Equifax 泄露 1.43 亿敏感征信记录
  - Java Struts 漏洞致 2/3 美国成年人社保、驾照、住址、信用卡等敏感信息泄露

Cybersecurity Incident & Im

Consumer Notice FAQs Potential Impact Enroll Trust

A Progress Update for Consumers

September 13, 2017

1) Updated information on U.S. website application vulnerabi

Equifax has been intensely investigating the scope of the intrusion wit
information was accessed and who has been impacted. We know tha
Apache Struts CVE-2017-5638. We continue to work with law enforce
with law enforcement.

2) Temporary interruption to credit freeze sign-up link.

sina 新浪财经 新浪财经 > 美股> 正文

美国1.43亿人个人信息被泄露

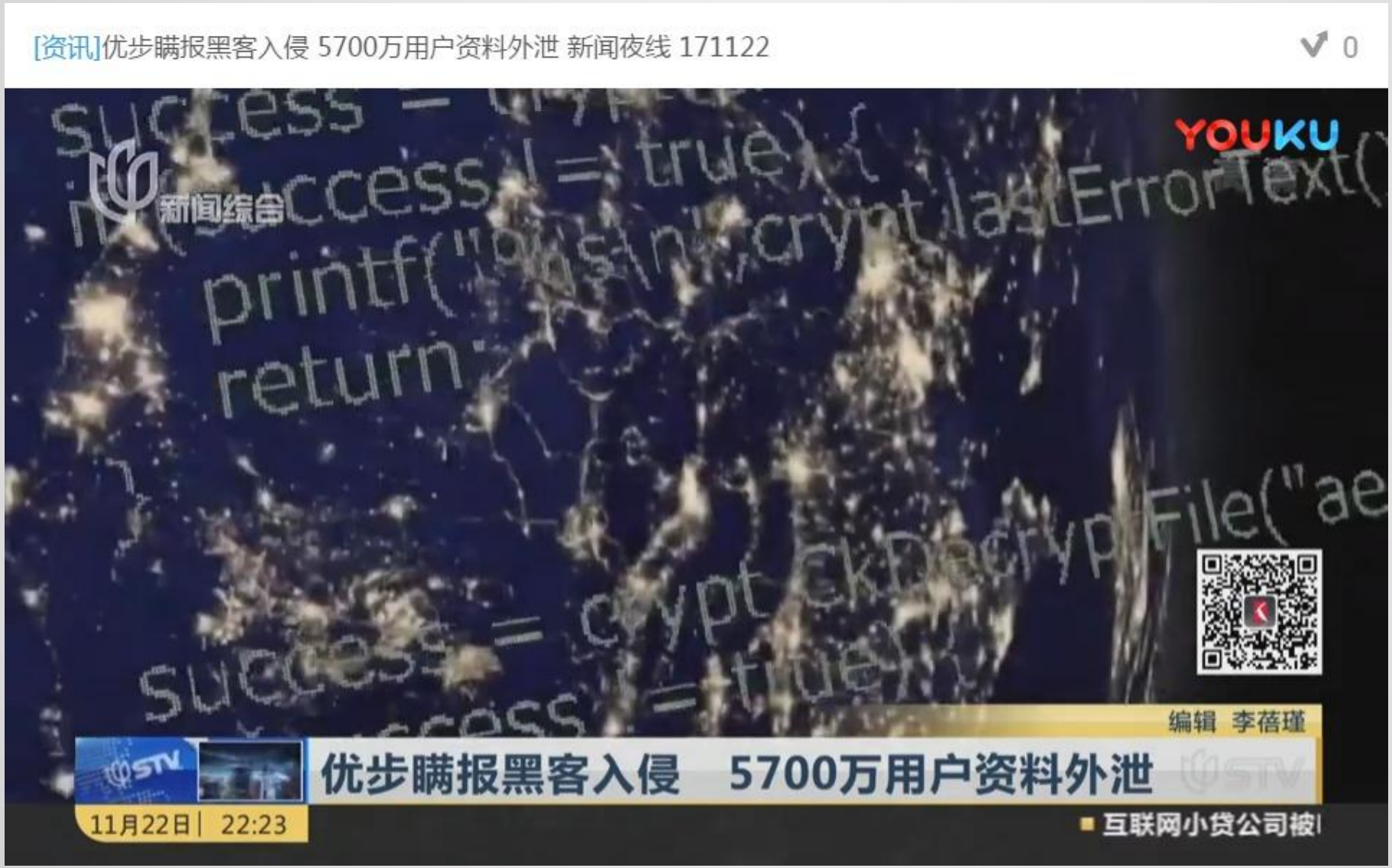
2017年09月08日 08:40 新浪科技 微博 暂有话说(10人参与) 收藏本文

美股行情中心：独家提供全美股行业板块、盘前盘后、ETF、权证实时行情

新浪科技讯 北京时间8日早间消息，美国征信企业Equifax披露称，其网站遭遇黑客攻击，造成1.43亿人的个人信息泄露，包括社会保障号码和驾照信息等。这可能是近年来最大的一起泄露事故。之前雅虎虽然泄露了10亿账户信息，但里面没有包含社会保障号和驾照信息。

白豚 WhiteDolphin

- 安全性补充说明 - 10: 优步 (Uber) 泄露 5700万用户资料



白豚
WhiteDolphin

•安全性补充说明 - 11: 微信支付“零元买买买”事故

- Java XML 组件 XXE 漏洞导致的微信支付“零元买买买”重大安全事故

www.news.cn 新华网 NEWS www.xinhuanet.com
让新闻离你更近

微信支付曝“0元购”漏洞 安全

2018-07-04 15:04:57 来源：新华

关注新华网

微信

微博

Qzone

0
评论

新华社厦门7月4日电（记者颜之宏）3日，有网络安全机构曝光了一组
技术漏洞，据称攻击者可利用该漏洞将自己伪装成微信支付平台，通过篡改
获得“0元购”特权。记者3日晚间从微信支付官方渠道获悉，该漏洞已修复，
度恐慌。

据网络安全专家谢忱介绍，从当前被公开的漏洞信息来看，网络攻击者
信支付官方SDK（软件工具开发包）存在的漏洞，将自己伪装成“微信支付平
通过微信的漏洞伪造与商户的直接通信，在篡改微信支付的正常通信信息后
换柱”的目的。

谢忱表示，正常的支付流程应该是由用户发起，经由微信支付平台到达
会有一个与微信支付平台确认支付结果的过程，而网络攻击者恰恰是利用了
“骗”过了商户。谢忱认为，一些商家的安全防护水平较低，攻击者还可通过
商户的密钥等信息，再通过这个漏洞就可以实现“将订单设置为0元”等操作，
导致该商户的消费者信息等数据内容泄漏。

网络支付安全专家于迪则认为，接入微信支付的商户不必过度恐慌。于迪表示，该

关于20180704微信支付漏洞的分析

kanmars
一个不懂生活的人，正在补习前半生的失误

+ 关注他

2 人赞了该文章

今天看新闻，说微信官方SDK有漏洞。

微信支付曝漏洞：可发伪造信息使购物无需付费

7月4日消息，近日有网友在国外安全社区发帖称微信支付官方SDK存在的严重漏洞，攻击者可通过此漏洞侵入商家服务器，获得商家关键安全密钥，通过发送伪造信息来欺骗商家而无需付费购买任何东西。

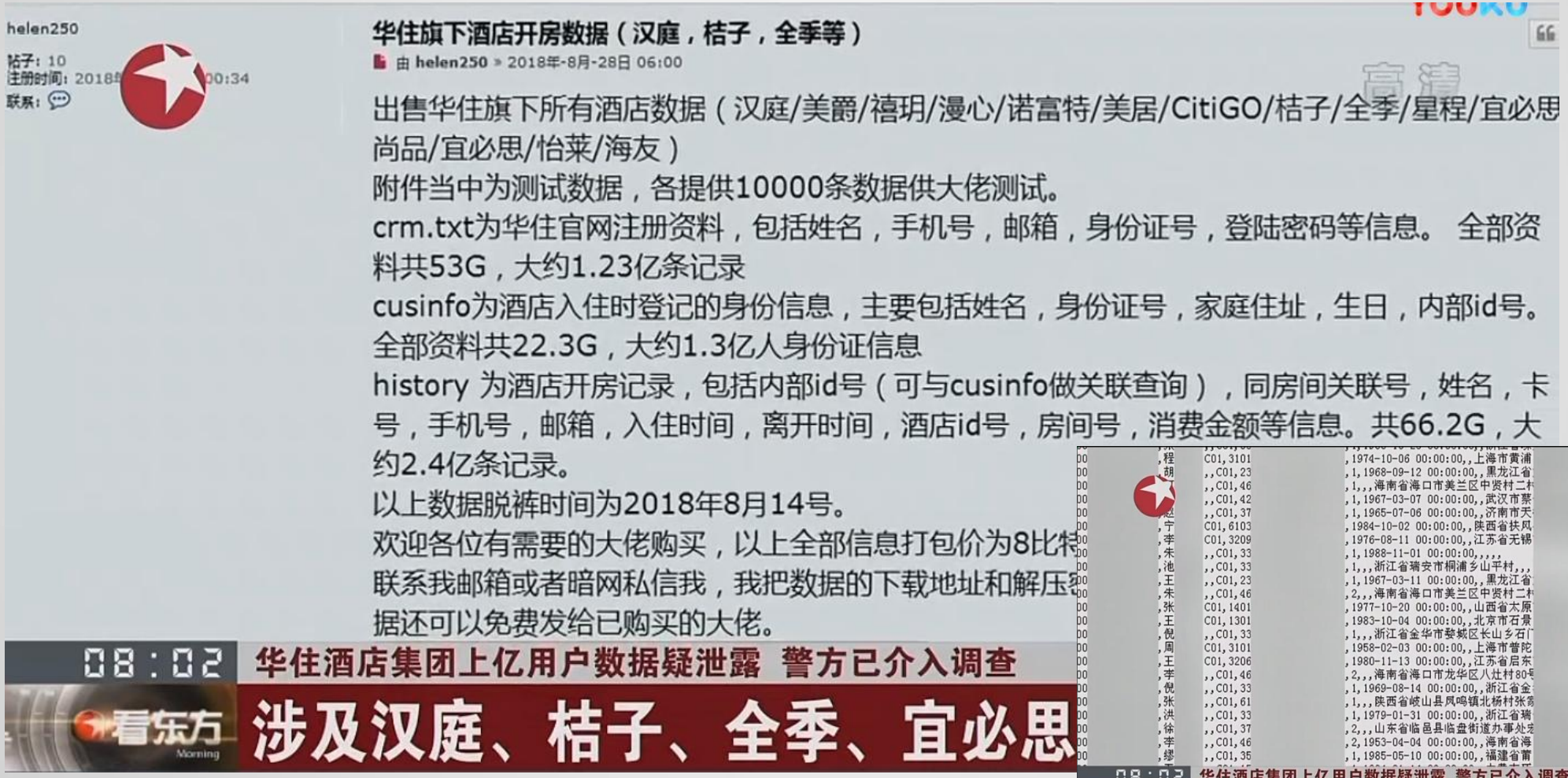
腾讯对此表示，微信支付技术安全团队已第一时间关注及排查，对官方网站上该SDK漏洞进行更新，修复了已知的安全漏洞，并在此提醒商户及时更新。

```
Example  vivo :
 attack:
    notify url:   https://pay.vivo.com.cn/webpay/wechat/callback.oo
          cmd: /home/

     result:
        tomcat

attack:
    notify url:   https://pay.vivo.com.cn/webpay/wechat/callback.oo
          cmd: /home/tomcat
    result:
```

WhiteDolphin

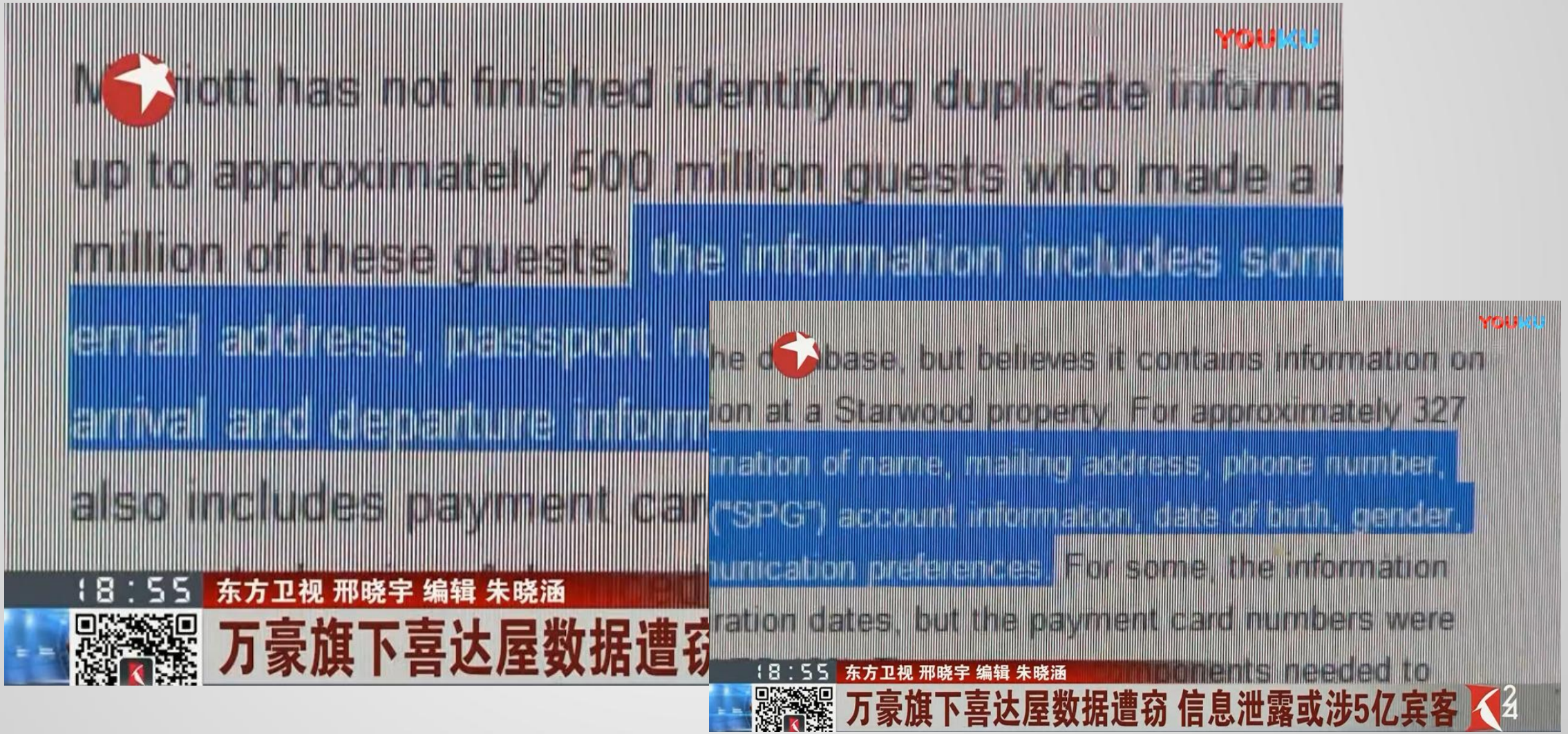
•安全性补充说明 - 12: 华住集团数亿客户信息泄露事故

- 华住集团汉庭、桔子等多家酒店泄露 1.3 亿人敏感信息和 2.4 亿开房记录



•安全性补充说明 - 13: 万豪集团数亿客户信息泄露事故

- 万豪集团喜来登、威斯汀、W等多家酒店泄露 5 亿人敏感信息和开房记录



重玄科技
PHILO-TECH