的全新的签名方案 APK Signature Scheme v2 中支持 SHA-2 家族的 SHA-256 和 SHA-512，但经过我们的验证，目前大量设备仍然在使用 sha1withRSA 的签名验证。在碰撞攻击的影响下，攻击者能够构造出内容篡改但是签名一致的文件绕过验证。尽管计算量巨大且对内容的控制存在一定的困难，但是我们认为这类安全机制已经不再可信。

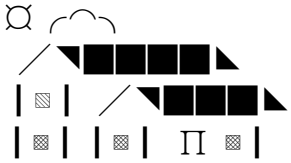
Google 公司和诸多 IT 安全研究人员均在过去几年呼唤开发者尽快更换 SHA-1 算法，早在 2014 年，Chrome 团队就已经宣布了淘汰 SHA-1 算法的时间表，本次碰撞实例的发布，也给所有还在持观望和犹豫态度的人敲响了警钟：赶紧为安全的系统启用新的 Hash 算法！

事实上，SHA-1 算法的后继算法早就已经被研究人员设计和推广，SHA-2 算法家族（包括六种 Hash 函数：SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256）在 2001 年就已经公布，而 NIST 在经过多年的 SHA-3 设计竞赛后，在 2015 年正式推荐由著名的密码学研究人员 Guido Bertoni, Joan Daemen, Michaël Peeters 和 Gilles Van Assche 共同设计的 Keecak 算法家族作为 SHA-3 的候选算法。更为值得注意的是，中国国家密码管理局同样在 2010 年底发布了我国自主的国密 SM3 消息摘要（密码杂凑）算法。这些算法的安全性在目前经受住了广泛的测试和分析，是值得信赖的。所以，文章的最后，GoSSIP 小组建议大家：任何以 SHA-1 作为消息摘要算法的安全产品应该尽快更换至这些更为安全的 Hash 算法。

供稿人：李成

» SIGDRM WEEKLY LETTERS «

» QQ：10006549 «



主　　编：张志勇
副 主 编：赵长伟
责任编辑：史培宁
网络校对：韩林茜

• D　R　M° •