固态硬盘的加密功能可以被绕过

非官方中文译文·安天技术公益翻译组 译注

简译版

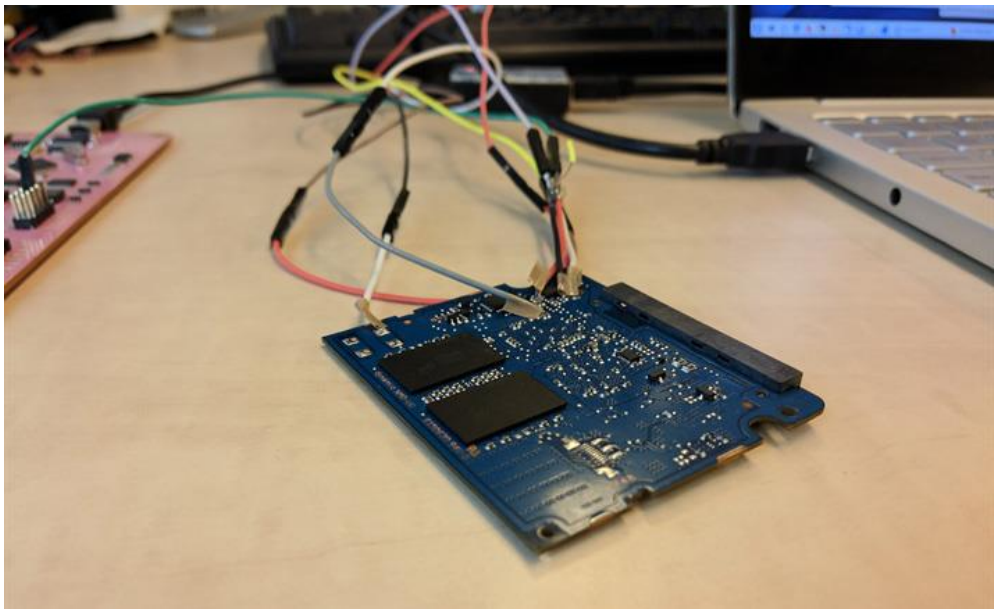
文档信息			
原文名称	Self-encrypting SSDs vulnerable to encryption bypass attacks		
原文作者	Zeljka Zorz	原文发布日期	2018 年 11 月 6 日
作者简介	Zeljka Zorz 是 Help Net Security 的总编辑。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2018/11/06/self-encrypting-ssds-vulnerable/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

固态硬盘的加密功能可以被绕过

Zeljka Zorz

2018 年 11 月 6 日

研究人员发现，英睿达（镁光旗下的子公司）和三星制造的几种固态硬盘（SSD）的硬件加密存在安全漏洞。攻击者可以利用这些漏洞，绕过硬盘的加密功能，从而访问硬盘中的数据——他们根本无需获取用户的硬盘加密口令。



调查结果

荷兰内梅亨大学（Radboud University）的卡罗·梅杰（Carlo Meijer）和伯纳德·范·加索尔（Bernard van Gastel）通过对 7 款固态硬盘的固件进行逆向工程，来分析它们的安全性。这 7 款硬盘分别是：英睿达 MX100、MX200 和 MX300（内置）；三星 840 EVO 和 850 EVO（内置）；三星 T3 和 T5（移动）。

这两家公司的其他类似新产品可能也存在漏洞，不过研究人员没有对它们进行测试和确认。但是，正如这两家公司所说，他们生产的 SSD 几乎占了全球销量的一半，因此修复这些漏洞至关重要。

“第一个漏洞是 CVE-2018-12037，它出现的原因是：最终用户的口令和用于加密用户数据的加密密钥之间没有加密绑定。因此，用户数据的机密性不依赖于加密机制。攻击者可

以在硬盘的控制器上执行代码来恢复用户数据（可以通过 JTAG、内存破坏、存储芯片内容操纵和故障注入等方法实现）。”研究人员在安全公告中解释道。

该漏洞会影响上述所有硬盘。但是有一点需要注意：只有在“高速”（High）模式下使用 ATA 安全加密时，三星 840 EVO 和 850 EVO 才会受到加密绕过和数据恢复攻击。

第二个漏洞是 CVE-2018-12038，它出现的原因是：一旦完成了加密操作，存储在已经磨损的存储芯片中的密钥信息就不能完全擦除了，因此攻击者可以访问这些信息。此漏洞会影响三星 840 EVO 硬盘。

研究人员还发现，Windows 系统使用的 BitLocker 加密工具也存在安全漏洞，“如果硬盘支持全盘加密，BitLocker 就会完全依赖硬件加密，而不再采取软件加密。因此，在这种硬盘中，由 BitLocker 保护的数据也会受到该漏洞的影响。”

关于研究人员的方法、发现和成功攻击的更多细节，可以参考其论文，但他们不会公布其漏洞利用工具。

如何应对？

2018 年 4 月，这两位研究人员本着负责任的态度，向英睿达和三星报告了他们的研究结果。

三星发布了用户通知，建议使用受影响移动硬盘的用户更新固件——用户可以自己更新，也可以到最近的三星服务中心寻求技术人员的帮助。对于非便携式硬盘（用于笔记本电脑、平板电脑和计算机），用户必须先进行软件加密，然后才能将数据存储在硬盘上，以保证数据的安全。

“我们建议用户安装与系统兼容的加密软件（在线免费软件）。”该公司建议道。

英睿达尚未对研究结果发表任何评论，尽管一些用户渴望获得关于漏洞处理的更多细节。

“为了保证数据的机密性，我们建议采用硬件加密的用户也使用软件全盘加密解决方案，最好是开源和经过审计的解决方案，特别是 VeraCrypt。这是因为 VeraCrypt 能够在操作系统运行时进行就地加密（in-place encryption），并且可以与硬件加密共存。”研究人员指出。

“如果用户使用 BitLocker 加密，则需要设置组策略，这会阻止它通过 TCG Opal 加密新硬盘——转而使用软件加密。但是，这对已经部署的硬盘没有影响。只有新安装的硬盘，

包括正确设置组策略和完全擦除内置硬盘，才会被强制实施软件加密。鉴于 VeraCrypt 能够提供就地加密，它可以作为这些现有加密方案的替代方案。”

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*