Exim 服务器 BDAT 指令远程代码执行漏洞（CVE-2017-16943）通告

文档信息

编号	360TI-SV-2017-0017
关键字	CVE-2017-16943 CVE-2017-16944 Exim
发布日期	2017 年 12 月 13 日
更新日期	2017 年 12 月 15 日
TLP	WHITE
分析团队	360 威胁情报中心

通告背景

2017 年 11 月 23 日，流行邮件服务器程序 Exim 相关的两个漏洞被提交给 Exim Bugziliza，其中 CVE-2017-16943 为 UAF（Use After Free）类型漏洞，可能导致远程代码执行，CVE-2017-16944 可导致拒绝服务。11 月 25 日相应的 POC 被放出，但是该 POC 有限制，需要在特殊情况下才能触发。12 月 11 日，安全研究者发布了文章对漏洞进行了详细的技术分析，并证明利用 CVE-2017-16943 漏洞可实现远程代码执行。

360 威胁情报中心已根据重现漏洞，漏洞相关的技术细节已经公开，互联网上受影响的主机数目较多。此漏洞极有可能被利用来执行大规模的攻击，控制关键的邮件服务器，构成严重的现实威胁。

漏洞概要

漏洞名称	Exim 服务器 BDAT 指令远程命令执行漏洞（CVE-2017-16943）通告				
威胁类型	远程代码执行	**威胁等级**	高	**漏洞 ID**	CVE-2017-16943
漏洞利用场景					
攻击者远程主动连接访问存在漏洞的 Exim 服务器，无需用户验证发送恶意命令数据导致在服务器上执行恶意指令，获取对服务器的控制。					
受影响系统及应用版本					
Exim 4.88/4.89 并开启 chunking 选项					
不受影响系统及应用版本					
Exim 4.89.1 及以上版本					

漏洞描述

Exim 是由剑桥大学 Philip Hazel 开发的邮件传输代理，负责邮件的路由，转发和投递。它可运行在绝大多数的类 Unix 系统上，包括 Solaris、AIX、Linux、macOS 等。相比其他 MTA，Exim 配置更灵活，支持 String Expansion 技术，能执行诸如条件判断，字符转换等功能。

近期 Exim 被爆出两个漏洞：一个为 UAF（Use After Free）类型漏洞（CVE-2017-16943），可能被利用来执行任意指令；另一个为命令处理逻辑漏洞（CVE-2017-16944），可能导致拒绝服务。当 Exim 版本为 4.88 和 4.89 并开放 chunking（BDAT 指令）选项时，攻击者可通过发送恶意构造的字串触发对应漏洞，从而导致服务器远程代码执行或拒绝服务。

本通告重点关注可能导致远程代码执行的 CVE-2017-16943 漏洞，攻击者可以利用此漏洞无需用户验证通过发送带有畸形参数的 BDAT 命令在服务器上执行任意指令，从而完全控制邮件服务器。

影响面评估

360 威胁情报中心确认 CVE-2017-16943 漏洞可被利用来远程执行任意命令，漏洞影响 Exim 4.88 和 4.89 版本（需要开启 chunking 选项）。目前评估潜在受影响主机数量超过 300000 台（4.88 版本 120000+台，4.89 版本 180000+台），整体影响面较大，综合分析威胁等级为高。

处置建议

修复方法

1. 升级 Exim 到 4.89.1 及以上版本。
2. 如暂时无法升级服务器程序，作为临时解决方案，可在 config 里将 chunking_advertise_hosts 选项留空，使漏洞暂时无法被利用。

技术分析

CVE-2017-16943 为一个 UAF（Use After Free）类型漏洞，漏洞主要发生在函数 receive_msg 的以下代码中，这三个函数用于 Exim 中相关的堆操作：

1. store_extend 用于堆扩展
2. store_get 用于分配堆
3. store_release 用于释放堆

当用于解析 head 的 buffer 长度不够时，通过 stroe_extend 扩展 next->text，如果此时 stroe_extend 扩展失败，则通过 store_get 直接分配一段堆内存，并通过 stroe_releases 释放掉之前的 next->text 内存。

由于 Exim 中堆管理函数的问题，通过 BDAT 构造特殊的字符串，将导致 store_get 分配的内存为 next->text 指向的内存的子块，而在后续的函数 stroe_releases 中 next->text 指向的内存被释放，程序之后运行时复用将导致 UAF。

```
if (ptr >= header_size - 4)
  {
  int oldsize = header_size;
  /* header_size += 256; */
  header_size *= 2;
  if (!store_extend(next->text, oldsize, header_size))
    {
    uschar *newtext = store_get(header_size);
    memcpy(newtext, next->text, ptr);
    store_release(next->text);
    next->text = newtext;
    }
  }
```

使用 Meh 提供的 POC，运行之后可以看到对应处理的子进程已经崩溃，但是并不影响主进程，从对应的分析文章来看，作者已实现可用的远程命令执行。

```
a
**** debug string too long - truncated ****
03:41:18  3150 LOG: smtp_syntax_error MAIN
03:41:18  3150   **** log string overflowed log buffer ****
03:41:18  3150 SMTP>> 500 unrecognized command
03:41:18  3150 SMTP<< BDAT 1
03:41:18  3150 chunking state 1, 1 bytes
03:41:18  3150 search_tidyup called
03:41:18  3150 SMTP>> 250 1 byte chunk received
03:41:18  3150 chunking state 0
03:41:18  3150 SMTP<< BDAT
03:41:18  3150 LOG: smtp_protocol_error MAIN
03:41:18  3150   SMTP protocol error in "BDAT \177" H=localhost (test) [127.0.0.
1] missing size for BDAT command
03:41:18  3150 LOG: MAIN REJECT
03:41:18  3150   SMTP call from localhost (test) [127.0.0.1] dropped: too many s
yntax or protocol errors (last command was "BDAT \177")
03:41:18  3150 SMTP>> 501-missing size for BDAT command
03:41:18  3150 SMTP>> 501 Too many syntax or protocol errors
03:41:20  3136 child 3150 ended: status=0x8b
03:41:20  3136   signal exit, signal 11 (core dumped)
03:41:20  3136 0 SMTP accept processes now running
03:41:20  3136 Listening...
```

漏洞利用的细节详见参考资料节中 360CERT 的分析。

CVE-2017-16944 为一个可导致拒绝的漏洞，如下所示通过‘.’标记 email 的结束，代码中对 BDAT 命令的校验不标准，以至于 receive_getc 不会被重置，从而导致在后续函数 bdat_getc（）中的死循环，最终导致拒绝服务。

```
if (ptr == 0 && ch == '.' && (smtp_input || dot_ends))
  {
  ch = (receive_getc)(GETC_BUFFER_UNLIMITED);
  if (ch == '\r')
    {
    ch = (receive_getc)(GETC_BUFFER_UNLIMITED);
    if (ch != '\n')
      {
      receive_ungetc(ch);
      ch = '\r';               /* Revert to CR */
      }
    }
  if (ch == '\n')
    {
    message_ended = END_DOT;
    store_reset(next);
    next = NULL;
    break;                     /* End character-reading loop */
    }
```

参考资料

https://devco.re/blog/2017/12/11/Exim-RCE-advisory-CVE-2017-16943-en/
https://xorl.wordpress.com/2017/11/26/cve-2017-16943-exim-use-after-free/
https://xorl.wordpress.com/2017/12/02/cve-2017-16944-exim-bdat-infinite-loop-remote-dos/
https://bugs.exim.org/show_bug.cgi?id=2199
https://cert.360.cn/report/detail?id=9efc77a68170170bc490e876d4087fb2

更新历史

时间	内容
2017 年 12 月 13 日	初始报告
2017 年 12 月 15 日	漏洞可利用情况的更新