

Coremail 未授权远程代码执行 漏洞情报速报

——攻防驱动数据安全

8月21日

近日，赛博昆仑安全捕获到 coremail 的邮件处理模块存在远程代码执行漏洞，只需向任意邮箱发送一份邮件，即可导致 coremail 的服务端执行任意代码。

1. 漏洞详情

漏洞名称：Coremail 未授权远程代码执行

威胁程度：

Coremail 是一款大规模电子邮件系统，在国内有很广泛的应用，该漏洞针对 Coremail 漏洞利用简单，且漏洞利用后的攻击后效较强，建议有应用 Coremail 的用户对此漏洞进行关注。

处置建议：

- 1). 暂无补丁，可等待官方的正式补丁发布后，第一时间进行加固；
- 2). 加强对 Coremail 服务器主机的可疑命令和可疑网络外联行为的监测和响应；
- 3). 加强对 Coremail 邮箱账号登录和邮件被读取的监测和响应；
- 4). 使用赛博昆仑洞见产品对应用进行加固。

漏洞类型： 0Day

厂商： 广东盈世计算机科技有限公司

产品官网链接：<https://www.coremail.cn/>

影响范围： Coremail XT5/XT6 所有版本

漏洞所在功能模块： 邮件处理模块

漏洞攻击效果： 未授权远程代码执行

2. 漏洞原理

Coremail 的邮件处理功能存在溢出漏洞，利用该漏洞可导致未经授权的攻击者在邮件服务端执行任意代码。

该漏洞利用较为简单且隐蔽，只需向任意邮箱地址发送一封邮件，即可实现服务端 RCE，导致内网横向、任意邮箱登录和任意邮件查看。

3. 漏洞演示

1). 首先查看并确认 BuildID，演示 1 个主流的较新版本-20230419(ff23bf83)

```
This XML file does not appear to have any style information associated with it. The document tree is shown below.
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<result>
  <code>S_OK</code>
  <object name="var">
    <string name="version">Coremail Webmail Server Version 2023.1-cmXT5 build 20230419(ff23bf83)</string>
  </object>
</result>
```

2). 通过恶意脚本连接 Coremail 服务器达成远程命令执行

```
[coremail@VM-0-3-centos corefiles]$ id
id
uid=1000(coremail) gid=0(root) groups=0(root)
bash: history: : cannot create: No such file or directory
bash: history: : cannot create: No such file or directory
[coremail@VM-0-3-centos corefiles]$ uname -a
uname -a
Linux VM-0-3-centos 3.10.0-1160.88.1.el7.x86_64 #1 SMP Tue Mar 7 15:41:52 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
bash: history: : cannot create: No such file or directory
bash: history: : cannot create: No such file or directory
[coremail@VM-0-3-centos corefiles]$ /home/coremail/bin/sautil chkver --withC
/home/coremail/bin/sautil chkver --withC
Coremail Utilities Version 2023.1-cmXT5 build 20230419(ff23bf83) Copyright 2000-2020 Mailtech
Using COREMAIL_HOME -> /home/coremail
Versions of programs ->
```