MailDepot 2033 2.3.3022 Cross Site Scripting

Authored by Micha Borrmann, Thomas Engel | Site syss.de

Posted Nov 16, 2020

MailDepot version 2033 (2.3.3022) suffers from a cross site scripting vulnerability.

tags | exploit, xss
advisories | CVE-2020-26554
SHA-256 | f82776b6e406fc3d421c55e64c73955573843831dc5dcd361b30f289b3c99402 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Advisory ID:               SYSS-2020-037
Product:                   MailDepot
Manufacturer:              REDDOXX GmbH
Affected Version(s):       2033 (2.3.3022)
Tested Version(s):         2033 (2.3.3022)
Vulnerability Type:        Persistent Cross-site Scripting (CWE-79)
Risk Level:                High
Solution Status:           Open
Manufacturer Notification: 2020-10-01
Solution Date:             2020-11-11
Public Disclosure:         2020-11-13
CVE Reference:             CVE-2020-26554
Authors of Advisory:       Micha Borrmann, Thomas Engel (SySS GmbH)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Overview:

REDDOXX MailDepot is  an e-mail archiving solution  with many features
and an optional web browser user interface.

The manufacturer describes the product as follows (see [1]):

"The email  archiving solution  works independently  from the  type of
mail server, supports any type of  storage and can therefore be easily
integrated into any existing infrastructure."

Due to the improper  server-side invalidation of authentication tokens
when using  the logout  function, authentication  tokens can  still be
used.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Vulnerability Details:

The web-based application displays the entire content of HTML e-mails.
Also, external  resources like images  or JavaScript will  be executed
during the display of an e-mail. In addition, the subject field is not
sanitized and  allows the injection  of JavaScript code which  will be
executed when an e-mail is displayed.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Proof of Concept (PoC):

There are a lot of tools that generate HTML mails including JavaScript.

The following part in an HTML e-mail illustrates the security issue:

<img src="https://www.example.org/xss.png">
<script>alert("XSS Demonstration")</script>
<script src="https://www.example.org/xss.js"></script>

The subject of an e-mail may  contain the following code which will be
executed when the e-mail is viewed:

<img src=X onerror='alert("XSS Demonstration")'</script>

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Solution:

Install the provided hotfix 43-restproxy-usergui [2]

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclosure Timeline:

2020-09-30: Detection of the vulnerability
2020-10-01: Vulnerability reported to manufacturer
2020-10-04: CVE number assigned
2020-10-05: Manufacturer confirms vulnerability
2020-11-11: Hotfix was released by the vendor
2020-11-13: Public release of the security advisory

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

References:

[1] REDDOXX MailDepot Product Website
    https://www.reddoxx.com/en/products/archiving/
[2] REDDOXX Release Notes
    https://appliance.docs.reddoxx.com/de/release-notes/release-notes-version-2033-final-2-3-3022
[3] SySS Security Advisory SYSS-2020-037
    https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2020-037.txt
[4] SySS Responsible Disclosure Policy
    https://www.syss.de/en/responsible-disclosure-policy/

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Credits:

This security vulnerability was found by Micha Borrmann and Thomas
Engel of SySS GmbH.

E-Mail: micha.borrmann (at) syss.de
Public Key: https://www.syss.de/fileadmin/dokumente/PGPKeys/Micha_Borrmann.asc
Key Fingerprint: 38BD 7A9C 3EA9 39C5 33F9  94D0 CFC2 D5B0 8EE0 CBB9

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclaimer:

The information provided in this security advisory is provided "as is"
and without  warranty of any  kind. Details of this  security advisory
may  be  updated  in  order  to provide  as  accurate  information  as
possible. The latest version of this security advisory is available on
the SySS website.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Copyright:

Creative Commons - Attribution (by) - Version 3.0
URL: http://creativecommons.org/licenses/by/3.0/deed.en
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEEOL16nD6pOcUz+ZTQz8LVsI7gy7kFAl+uX28ACgkQz8LVsI7g
y7mHXw/+MxTvRKJu8QEKKVff/igU1nuKkqS+3iyfZT6bT+24UOWHf7RmWi+68b++
VxOS1M7kY2aKYf/UmZY3/aFAxWLpO6Ao7LtEAckE2RJaeUPVSx7+lstijXQxXH+X
```

Follow us on Twitter

Subscribe to an RSS Feed

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 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11secur1ty 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 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)

```
zwhAFwhqQ0tPUFzE1BqV0DypQ+tRHl7JsqD77rJq0jRVX3r3RoJvgcGrjEWdkwRs
+Xa9+rrAJrkNLcSYkZMTNowLNi4zfwpHkeWkDg9/fF1jklcT+sVl9h2TJR3lrL0x
0uVxnVN5gm46BvrEBc1rmUbIYaecwCtRiSDkYx1luRTxlh1VduU2IU0i4RThGm9N
jPSB5bCBOxmgHaMHdNcAwlzYJmx35+Qe/zMlE3TRUr0Vj88aBAyPxTkHsgKa6F18
N7EU9a9Io8JAolW1bUDWvPHUKoLLA/2onn6aBhNgdZQGvHVZEHt9JvrgWueER6Yf
++0qyhEslzBwHXPJfgMj4lwr7OpGK8593FA1khpWvHtS3tj3RDSsQwWQ7RsarLaj
9YYz3i/0qS6w1x3zpOZQKSAb1vk6vS6q+s34vVsel9RI2ZY3cpzKEhUPy/z58XHC
D34SJWjUzKMVf0vDE8u1BV6oU8sGATChjP5VGsVoW+bBytKtHAHo/RLq09Y0DMJE
koAUadCa6IxusM0pprxf7ffxm+V5rr0K4KUbKFLl5HHsz/nEx+U=
=d596
-----END PGP SIGNATURE-----
```

Login or Register to add favorites

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