Advisory: ActFax 7.10 Build 0335 Privilege Escalation (CVE-2020-15843)

gepostet am 22.09.2020 von Dimitri Lesy (https://blog.to.com/author/dimitri-lesy/)

Während eines Penetrationstests ist mir aufgefallen, dass ActFax 7.10 Build 0335 in der Standardkonfiguration eine Sicherheitslücke enthält. Nach der Installation verfügt die Benutzergruppe „Everyone“ über die vollständige Kontrolle des „Terminal“ Verzeichnisses. Hierdurch kann jeder angemeldeter Benutzer alle Dateien des Verzeichnisses manipulieren. Diese Berechtigungskonfiguration kann zu einer Privilege Escalation führen.

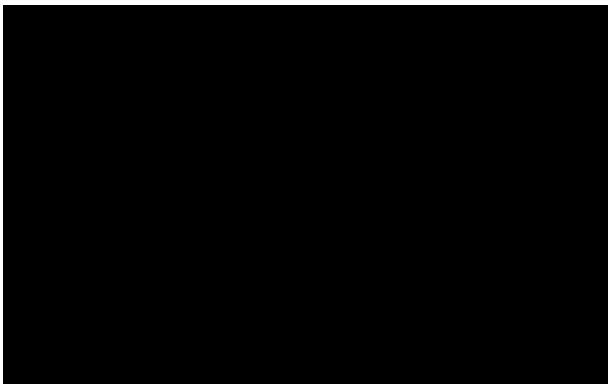
Detailed Security Advisory

Advisory ID: TO-2020-002
Product: ActFax (https://www.actfax.com/)
Vendor: ActFax Communication-Software GmbH (Krems an der Donau, Austria)
Tested Version: 7.10 Build 0335
Fixed Version: 7.15 Build 0342
Vulnerability Type: Privilege Escalation caused by incorrect default permissions
CVSSv2 Severity: AV:L/AC:M/Au:S/C:C/I:C/A:C (Score 6.6)
CVSSv3 Severity: AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H (Score 8.2)
Mitigation: Installation of the software upgrade provided by the vendor
CWE Reference: CWE-276
CVE Reference: CVE-2020-15843
Author: Dimitri Lesy, Thinking Objects GmbH

Overview

ActFax Version 7.10 Build 0335 (2020-05-25) is susceptible to a privilege escalation vulnerability due to **insecure folder permissions** on `%PROGRAMFILES%\ActiveFax\Client\`, `%PROGRAMFILES%\ActiveFax\Install\` and `%PROGRAMFILES%\ActiveFax\Terminal\`. The folder permissions allow „Full Control“ to „Everyone“. An authenticated local attacker can **exploit this** to replace the *TSClientB.exe* binary in the Terminal directory, which is executed on logon for every user. Alternatively, the attacker can **replace any of the binaries** in the Client or Install directories. The latter requires additional user interaction, for example starting the client.

Proof of Concept



Description of the steps taken in the Proof of Concept video above:

1. Using an administrative account, ActFax 7.10 Build 0335 is installed.
2. The administrator logs off.
3. A regular user (without administrative permissions) logs on.
   This could be an attacker.
4. The incorrect folder permissions of the „Terminal“ folder are shown.
5. The „TSClientB.exe“ binary is replaced with a binary containing a reverse shell to an attacking linux VM.
6. The user logs off.
7. A netcat listener is started in the Linux VM.
8. The administrator logs in once more.
9. Instead of the original „TSClientB.exe“ the attacker’s EXE-file is launched in the background.
10. The attacker receives a reverse shell connection from the victim, giving them administrative access to the system.

Remediation

ActFax version 7.15 Build 0342, released on the 14th of September 2020, sets correct permissions on the „Terminal“, „Install“, and „Client“ folders for both new and existing installations. The **corrected default permissions** do not allow „Everyone“ to modify the folders or their contents, therefore mitigating the privilege escalation vulnerability.

Disclosure Timeline

2020-07-07: Vulnerability discovered
2020-07-17: CVE reserved
2020-07-20: Vulnerability reported to the vendor.
2020-07-20: Vendor response, a patched version of the software will be released in September.
2020-07-21: The vendor supplied a beta version which should fix the problem for both existing and new installations.
2020-07-21: Confirmed that the vulnerability no longer exists for the „Terminal“ folder in the beta version. However, previously overlooked folders with the same issue were found.
2020-07-22: Informed the vendor of the previously overlooked folders.
2020-07-28: The vendor confirms that they discovered the same issue with the other folders during internal testing. A beta version mitigating the problem for every folder is made available.
2020-09-03: The vendor notified me of the planned release date (2020-09-14).
2020-09-14: The vendor released the patched version (7.15 Build 0342).
2020-09-21: Advisory published.

> ***I would like to thank the ActFax team for their quick and professional communication through the entire timeline.***

References

[1] Advisory URL: https://blog.to.com/advisory-actfax-7-10-build-0335-privilege-escalation-cve-2020-15843 (https://blog.to.com/advisory-actfax-7-10-build-0335-privilege-escalation-cve-2020-15843)
[2] ActFax Website: https://www.actfax.com/ (https://www.actfax.com/)

Disclaimer

Autor/in

Dimitri Lesy
(https://blog.to.com/author/dimitri-lesy/)

IT Security Consultant

Top Blogbeiträge

Wissen Sie, was auf ihrer Firewall vor sich geht?(https://blog.to.com/firewall-carewoche-regelwerk-review/)

Corona-Warn-App – Welche Daten werden geteilt?(https://blog.to.com/corona-warn-app-daten/)

Vulnerability Scan – Grenzen und Chancen(https://blog.to.com/vulnerability-scan-pt-2/)

Dies könnte Sie auch interessieren

Advisory: SuperWebMailer < 7.40.0.01550 Unauthenticated Remote Code Execution (CVE-2020-11546)
Die Versionen vor 7.40.0.01550 des SuperWebMailer sind anfällig für eine Remote Code Execution Sicherheitslücke (RCE). Die Anwendung verarbeitet die Language-Variable ohne ausreichende Sicherheitsprüfung und reicht diese intern in ein eval(), was einem unauthentifizierten Angreifer die Ausführung von beliebigem PHP Code im Kontext des Webservers erlaubt (CWE-94). Die Sicherheitslücke ist laut Hersteller in Version 7.40.0.01550 behoben worden (8.4.2020).

(https://blog.to.com/advisory-superwebmailer-cve-2020-11546/)

Wie wird man Penetrationstester?
Bei einem Penetrationstest (oft Pentest genannt) testen Penetrationstester, auch Ethical Hackers genannt, die Sicherheit eines IT-Systems. Dabei kann es sich z. B. um ein Computernetzwerk, eine Website oder eine Smartphone-App handeln. Ziel ist das frühzeitige Identifizieren von Schwachstellen in dem System, um es danach gegen Angreifer schützen zu können.

(https://blog.to.com/penetrationstester/)

Schreibe einen Kommentar

Deine E-Mail-Adresse wird nicht veröffentlicht. Erforderliche Felder sind mit * markiert.

KOMMENTAR

NAME *

E-MAIL *

WEBSITE

MEINEN NAMEN, E-MAIL UND WEBSITE IN DIESEM BROWSER SPEICHERN, BIS ICH WIEDER KOMMENTIERE.

CAPTCHA *

+ = II

Kommentar abschicken

(https://www.xing.com/companies/thinkingobjectsgmbh) (https://de.linkedin.com/company/thinking-objects-gmbh) (https://twitter.com/thinkingobjects)

(https://www.youtube.com/channel/UCvkXLivj61AEbZs3Wh49L5w) (https://www.facebook.com/TopalisGruppe)