CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-024

Multiple Vulnerabilities in the Autodesk FBX Library

April 24, 2020 — v1.0

TLP:WHITE

History:

- *24/04/2020 — v1.0 – Initial publication*

Summary

On April 15, 2020, Microsoft has announced the release of updates to address multiple vulnerabilities found in the Autodesk FBX library which is integrated into certain Microsoft applications such as Microsoft Office, Office 365 ProPlus and Paint 3D [1].

Applications and services that utilize the FBX-SDK Ver. 2020.0 or earlier can be impacted by buffer overflow, type confusion, use-after-free, integer overflow, NULL pointer dereference, and heap overflow vulnerabilities. This can lead to remote code execution.

Technical Details

Remote code execution vulnerabilities exist in Microsoft products that utilize the FBX library when processing specially crafted 3D content. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

To exploit the vulnerabilities, an attacker must send a specially crafted file containing 3D content to a user and convince them to open it.

The details of the vulnerabilities are as follows [2]. A user may be tricked into opening a malicious FBX file which may exploit:

- a buffer overflow vulnerability in FBX's SDK causing it to run arbitrary code on the system (CVE-2020-7080) [3];
- a type confusion vulnerability in FBX's SDK causing it to read/write out-of-bounds memory location or run arbitrary code on the system or lead to denial-of-service (CVE-2020-7081);
- a use-after-free vulnerability in FBX's SDK causing the application to reference a memory location controlled by an unauthorized third party, thereby running arbitrary code on the system (CVE-2020-7082);

- an integer overflow vulnerability in FBX's SDK causing the application to crash leading to a denial of service (CVE-2020-7083);
- a null pointer dereference vulnerability in FBX's SDK causing the application to crash leading to a denial of service (CVE-2020-7084);
- the heap overflow vulnerable FBX parser to obtain a limited code execution by altering certain values in a FBX file, causing the application to run arbitrary code on the system (CVE-2020-7085).

Products Affected

- Microsoft Products: Office 365 ProPlus for 32 and 64-bit Systems, Microsoft Office 2019 for 32 and 64 bit editions and Paint 3D

- Also the following third party software:
  - FBX-SDK version 2019.5 and earlier,
  - Maya version 2019 and earlier,
  - Motion Builder version 2019 and earlier,
  - Mudbox version 2019 and earlier,
  - 3ds Max version 2020 and earlier,
  - Fusion version ATF 8 and earlier,
  - Revit version 2020 and earlier,
  - Flame version 2019 and earlier,
  - Infraworks version 2020 and earlier,
  - Navisworks version 2019 Update 4 and earlier,
  - Autodesk AutoCAD version 2019 and earlier.

Recommendations

The security updates that were released, address these vulnerabilities by correcting the way 3D content is handled by Microsoft software. Although the out-of-band advisory was published this week, patches for the Microsoft affected software are expected to arrive as part of May's Patch Tuesday.

CERT-EU highly recommends the upgrade to the latest version via Microsoft Update, Autodesk Desktop App or the Accounts Portal. For third party developers who use the FBX-SDK in their applications or services, CERT-EU highly recommends they obtain and apply the latest version of the FBX-SDK from the official update source.

References

[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200004

[2] https://www.autodesk.com/trust/security-advisories/adsk-sa-2020-0002

[3] https://nvd.nist.gov/vuln/detail/CVE-2020-7080