مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Multiple ZDI Vulnerabilities in Autodesk AutoCAD

Tracking #:432315975

Date:24-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Autodesk AutoCAD and certain AutoCAD-based products are affected by multiple vulnerabilities that could allow remote attackers to execute arbitrary code.

TECHNICAL DETAILS:

Autodesk AutoCAD and certain AutoCAD-based products are affected by Out-of-Bounds Write, Out-of-Bounds Read, Heap-based Overflow, Use-After-Free, Memory Corruption, and Uninitialized Variable vulnerabilities.
These vulnerabilities only impact the Windows versions of Autodesk AutoCAD and related products. Other platforms, such as macOS or Linux, are not affected. Exploitation of these vulnerabilities may lead to code execution and requires user interaction for exploitation.

Vulnerabilities Details:

- CVE-2024-23150: A maliciously crafted PRT file, when parsed in odxug_dll.dll through Autodesk applications, can force an Out-of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
- CVE-2024-23151: A maliciously crafted 3DM file, when parsed in ASMkern229A.dll through Autodesk applications, can force an Out-of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
- CVE-2024-23152: A maliciously crafted 3DM file, when parsed in opennurbs.dll through Autodesk applications, can force an Out-of-Bounds Read. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
- CVE-2024-23153: A maliciously crafted MODEL file, when parsed in libodx.dll through Autodesk applications, can force an Out-of-Bounds Read. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
- CVE-2024-23154: A maliciously crafted SLDPRT file, when parsed in ODXSW_DLL.dll through Autodesk applications, can be used to cause a Heap-based Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.
- CVE-2024-23155: A maliciously crafted MODEL file, when parsed in atf_asm_interface.dll through Autodesk applications, can be used to cause a Heap-based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash or execute arbitrary code in the context of the current process.
- CVE-2024-23156: A maliciously crafted 3DM file, when parsed in opennurbs.dll and ASMkern229A.dll through Autodesk applications, can lead to a memory corruption vulnerability by write access violation. This vulnerability, along with other vulnerabilities, can lead to code execution in the current process.
- CVE-2024-23157: A maliciously crafted SLDASM or SLDPRT file, when parsed in ODXSW_DLL.dll through Autodesk applications, can lead to a memory corruption vulnerability by write access violation. This vulnerability, along with other vulnerabilities,

can lead to code execution in the current process.

- CVE-2024-23158: A maliciously crafted IGES file, when parsed in ASMImport229A.dll through Autodesk applications, can be used to cause a use-after-free vulnerability. A malicious actor can leverage this vulnerability to cause a crash or execute arbitrary code in the context of the current process.
- CVE-2024-23159: A maliciously crafted STP file, when parsed in stp_aim_x64_vc15d.dll through Autodesk applications, can be used to uninitialized variables. This vulnerability, along with other vulnerabilities, can lead to code execution in the current process.
- CVE-2024-36999: A maliciously crafted 3DM file, when parsed in opennurbs.dll through Autodesk applications, can force an Out-of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.

Affected Products:

Product	Impacted Versions
Autodesk AutoCAD, AutoCAD Architecture	2024
Autodesk AutoCAD Electrical, AutoCAD Map 3D	2024
Autodesk AutoCAD Mechanical, AutoCAD MEP	2024
Autodesk AutoCAD Plant 3D, Autodesk Civil 3D	2024
Autodesk Advance Steel	2024

Mitigations:

- Refrain from using the IMPORT feature
- Disable imports of the following file types by renaming acTranslators.exe in the product install folder: CATPART, SLDASM, X_B, 3DM, CATPROD, STP, MODEL, SLDDRW, SLDPRT, X_T
- Import files from trusted sources only

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the mitigations now and install the fixed versions on upcoming release.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010