VDB-308284 · CVE-2025-4539 · GCVE-100-308284

HAINAN TODESK 4.7.6.3 DLL FILE PARSER PROFAPI.DLL UNCONTROLLED SEARCH PATH

A vulnerability was found in Hainan ToDesk 4.7.6.3. It has been declared as critical. This vulnerability affects an unknown code in the library *profapi.dll* of the component *DLL File Parser*. The manipulation with an unknown input leads to a uncontrolled search path vulnerability. The CWE definition for the vulnerability is CWE-427. The product uses a fixed or controlled search path to find resources, but one or more locations in that path can be under the control of unintended actors. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared for download at yuque.com. This vulnerability was named CVE-2025-4539. The exploitation appears to be difficult. The attack needs to be approached locally. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1574.

It is possible to download the exploit at yuque.com. It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entries VDB-291476, VDB-292528, VDB-293510 and VDB-293511 are related to this item.

Product

Vendor

- Hainan

Name

- ToDesk

Version

- 4.7.6.3

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 7.0
VulDB Meta Temp Score: 6.7

VulDB Base Score: 7.0
VulDB Temp Score: 6.4
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 7.0
CNA Vector: 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Uncontrolled search path
CWE: CWE-427 / CWE-426
CAPEC: 🔒
ATT&CK: 🔒

Local: Yes
Remote: No

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/10/2025		Advisory disclosed
05/10/2025	+0 days	VulDB entry created
05/11/2025	+1 days	VulDB entry last update

Sources

Advisory: yuque.com
Status: Not defined

CVE: CVE-2025-4539 (🔒)
GCVE (CVE): GCVE-0-2025-4539
GCVE (VulDB): GCVE-100-308284
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/10/2025 03:04 PM
Updated: 05/11/2025 01:35 PM
Changes: 05/10/2025 03:04 PM (56), 05/11/2025 01:35 PM (30)
Complete: 🔍

Submitter: Ba1_Ma0
Cache ID: 5:7FF:101

Submit

Accepted

- Submit #566698: Hainan Interesting Technology Co., Ltd todesk 4.7.6.3 privilege escalation (by Ba1_Ma0)

Discussion

No comments yet. Languages: en.

Please log in to comment.