VDB-308277 · CVE-2025-4532 · GCVE-100-308277

SHANGHAI BAIRUI INFORMATION TECHNOLOGY SUNLOGINCLIENT 15.8.3.19819 SUNLOGIN_GUARD.EXE UNCONTROLLED SEARCH PATH

A vulnerability classified as critical has been found in Shanghai Bairui Information Technology SunloginClient 15.8.3.19819. This affects an unknown code in the library *process.dll* of the file *sunlogin_guard.exe*. The manipulation with an unknown input leads to a uncontrolled search path vulnerability. CWE is classifying the issue as 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. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared at yuque.com. This vulnerability is uniquely identified as CVE-2025-4532. The exploitability is told to be difficult. An attack has to be approached locally. Technical details and a public exploit are known. MITRE ATT&CK project uses the attack technique T1574 for this issue.

The exploit is shared for download 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.

Product

Vendor

- Shanghai Bairui Information Technology

Name

- SunloginClient

Version

- 15.8.3.19819

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: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

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-2025-4532 (🔒)
GCVE (CVE): GCVE-0-2025-4532
GCVE (VulDB): GCVE-100-308277
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 05/10/2025 07:51 AM
Updated: 05/11/2025 09:03 AM
Changes: 05/10/2025 07:51 AM (56), 05/11/2025 09:03 AM (30)
Complete: 🔍
Submitter: Ba1_Ma0
Cache ID: 5:B87:101

Submit

Accepted

- Submit #566141: Shanghai Bairui Information Technology Co., Ltd SunloginClient 15.8.3.19819 privilege escalation (by Ba1_Ma0)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2025 vuldb.com · cc by-nc-sa