



VDB-355297 · CVE-2026-5544 · GCVE-100-355297

UTT HIPER 1250GW UP TO 3.2.7-210907-180535 FORMREMOTECONTROL PROFILE STACK- BASED OVERFLOW

CVSS Meta Temp Score

8.0

Current Exploit Price (≈)

\$0-\$5k

CTI Interest Score

2.81-

Summary

A vulnerability was found in [UTT HiPER 1250GW up to 3.2.7-210907-180535](#). It has been classified as **critical**. This affects an unknown function of the file `/goform/formRemoteControl`. This manipulation of the argument `Profile` causes stack-based overflow. This vulnerability is tracked as [CVE-2026-5544](#). The attack is possible to be carried out remotely. Moreover, an exploit is present.

Details

A vulnerability has been found in [UTT HiPER 1250GW up to 3.2.7-210907-180535](#) and classified as **critical**. Affected by this vulnerability is an unknown code block of the file `/goform/formRemoteControl`. The manipulation of the argument `Profile` with an unknown input leads to a stack-based overflow vulnerability. The CWE definition for the vulnerability is [CWE-121](#). A stack-based buffer overflow condition is a condition where the buffer being overwritten is allocated on the stack (i.e., is a local variable or, rarely, a parameter to a function). As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared at [github.com](#). This vulnerability is known as [CVE-2026-5544](#). The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known.

It is possible to download the exploit at [github.com](#). It is declared as proof-of-concept.

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

The entries [VDB-328068](#), [VDB-339350](#) and [VDB-349645](#) are pretty similar.

Product

Vendor

- [UTT](#)

Name

- [HiPER 1250GW](#)

Version

- [3.2.7-210907-180535](#)

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 8.8

VulDB Meta Temp Score: 8.0

VulDB Base Score: 8.8

VulDB Temp Score: 8.0

VulDB Vector: 

VulDB Reliability: 

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Stack-based overflow

CWE: [CWE-121](#) / [CWE-119](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

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

- 04/04/2026 | Advisory disclosed
- 04/04/2026 | +0 days | VulDB entry created

04/04/2026

+0 days

VulDB entry last update

Sources

Advisory: [github.com](#)

Status: Not defined

CVE: [CVE-2026-5544](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5544](#)

GCVE (VulDB): [GCVE-100-355297](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

Entry

Created: 04/04/2026 09:01 AM

Changes: 04/04/2026 09:01 AM (55)

Complete: 🔍

Submitter: [cosy](#)

Cache ID: 172:ACD:179

Submit

Accepted

- [Submit #782268](#): UTT HiPER 1250GW <= v3.2.7-210907-180535 Buffer Overflow (by cosy)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)