VDB-308048 · CVE-2025-4440 · GCVE-100-308048

H3C GR-1800AX UP TO 100R008 /GOFORM/ASPFORM ENABLEIPV6 PARAM BUFFER OVERFLOW

A vulnerability was found in H3C GR-1800AX up to 100R008 and classified as critical. Affected by this issue is the function `EnableIpv6` of the file */goform/aspForm*. The manipulation of the argument `param` with an unknown input leads to a buffer overflow vulnerability. Using CWE to declare the problem leads to CWE-120. The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow. Impacted is confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability is handled as CVE-2025-4440. The exploitation is known to be easy. Access to the local network is required for this attack to succeed. Technical details as well as a public exploit are known.

The exploit is available 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.

See VDB-230430, VDB-230431, VDB-230432 and VDB-230433 for similar entries.

Product

Vendor

- H3C

Name

- GR-1800AX

Version

- 100R008

License

- commercial

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: 8.0
VulDB Meta Temp Score: 7.6

VulDB Base Score: 8.0
VulDB Temp Score: 7.3
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 8.0
CNA Vector: 🔒

CVSSv2

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

Exploiting

Class: Buffer overflow
CWE: CWE-120 / CWE-119
CAPEC: 🔒
ATT&CK: 🔒

Local: No
Remote: Partially

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

05/08/2025		Advisory disclosed
05/08/2025	+0 days	VulDB entry created
05/09/2025	+1 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4440 (🔒)
GCVE (CVE): GCVE-0-2025-4440
GCVE (VulDB): GCVE-100-308048
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/08/2025 06:57 PM
Updated: 05/09/2025 12:45 PM
Changes: 05/08/2025 06:57 PM (56), 05/09/2025 12:45 PM (39)
Complete: 🔍
Submitter: BabyShark
Cache ID: 5:22A:101

Submit

Accepted

- Submit #557087: New H3C Technologies Co., Ltd. H3C GR-1800AX <=100R008 Command execution (by BabyShark)

Discussion

No comments yet. Languages: en.

Please log in to comment.