






<div> bzyo add bigantsoft url ...</div> <div>on Apr 3</div> <div>History</div>	
..	
 imgs	8 months ago
 .gitkeep	8 months ago
 README.md	8 months ago

 README.md

# Vulnerability

---

BigAnt Server Version 5.6.06 suffers from Exposure of Sensitive Information to an Unauthorized Actor

# Prerequisites

---

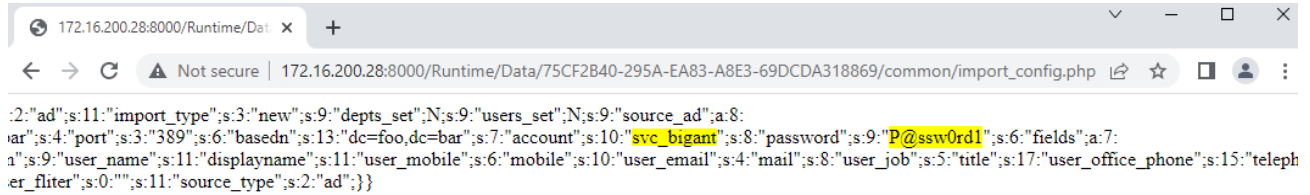
None

# Exploit

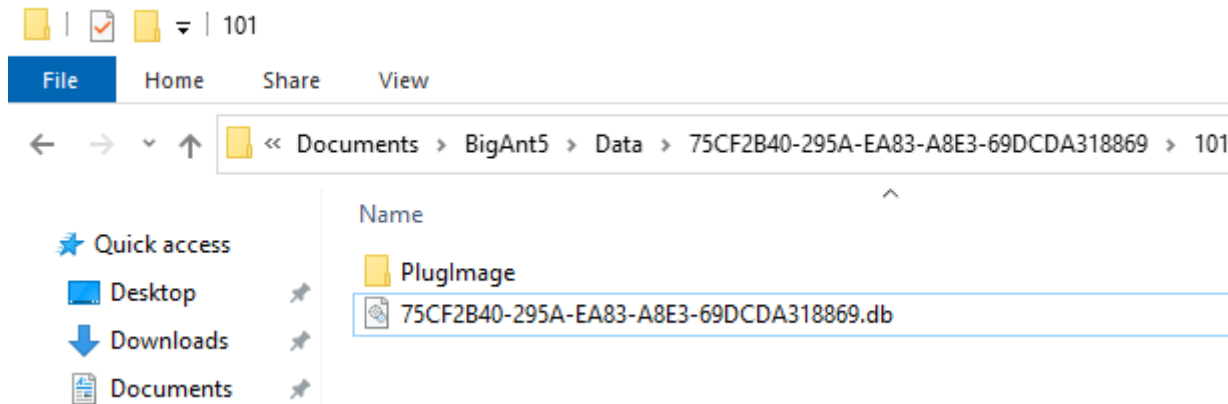
---

Combined with improper Access control, account information used to import AD/LDAP users can be accessed via the following URL by any non-authenticated user in cleartext

`http://<IPAddress:8000/Runtime/Data/75CF2B40-295A-EA83-A8E3-69DCDA318869/common/import_config.php`



\*Note the GUID is unique to the server install. This GUID can of course be brute forced or if you have a regular user login via the client, this GUID is populated under the user profile `C:\Users\<username>\Documents\BigAnt5\Data\75CF2B40-295A-EA83-A8E3-69DCDA318869\<bigantuser_id>`



## 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

# Disclaimer

---

Content is for educational and research purposes only. Author doesn't hold any responsibility over the misuse of the software, exploits or security findings contained herein and does not condone them whatsoever.