

master cve-pocs / CVE-2022-23349 /



bzyo add bigantsoft url ...

on Apr 3 History

..



.gitkeep

8 months ago



README.md

8 months ago

☰ README.md

Vulnerability

BigAnt Server Version 5.6.06 suffers from Cross Site Request Forgery (CSRF)

Prerequisites

Requires administrator to go to specially crafted URL

Exploit

Administrator account is created by going to or clicking on a specially crafted URL

bigant-csrf.mp4

0:00 / 1:02

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-2022-23349](#)
[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.