

master [cve-pocs / CVE-2022-26281 /](#)



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 Sensitive Cookie Without 'HttpOnly' Flag

Prerequisites

None

Exploit

Administrator PHP Session ID does not have HttpOnly or Secure checked

The screenshot shows the BigAnt Administration web interface. The top navigation bar includes 'Console Home', 'Users', 'System Settings', 'System Tools', 'App Add-ins', 'Database management', 'Security Control', and 'Server Logs'. The main content area displays 'Welcome: Super Admin' with a disk usage indicator. Below this are sections for 'Short cuts', 'User guide', and 'Recommended reading'. The bottom section shows the 'Application' tab with a table of cookies.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	SameParty	Priority
saas	default	localhost	/	2022-02-28T22:09:53.866Z	11	✓				Medium
account	superadmin	localhost	/	2022-02-28T22:09:53.866Z	17	✓				Medium
PHPSESSID	pbgr3ht3hk1j8iegr8jknosb	localhost	/	Session	35					Medium

Below the table, there is a button labeled 'Select a cookie to preview its value'.

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
 03-28-2022: PoC/CVE published

Reference

[MITRE CVE-2022-26281](#)

[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.