Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Unpatched Flaws Let Hackers Take Over BigAnt Server

Date of Publication	Admiralty Code	TA Number
March 5, 2025	A1	TA2025064

Summary

First Seen: February 3, 2025
Affected Product: BigAntSoft BigAnt Server
Impact: Two critical vulnerabilities, CVE-2025-0364 and, CVE-2024-54761 have been discovered in BigAnt Server. While CVE-2024-54761 was initially misclassified, further analysis uncovered CVE-2025-0364, which lets unauthenticated attackers bypass CAPTCHA to create admin accounts and execute arbitrary PHP code via the Cloud Storage Addin, risking full system compromise. No official patch is available yet, and public exploits exist, making immediate mitigations such as disabling SaaS registration and restricting access essential.

⚙ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-0364	BigAntSoft BigAnt Server Authentication Bypass Vulnerability	BigAntSoft BigAnt Server	✓	✗	✗
CVE-2024-54761	BigAntSoft BigAnt Office Messenger SQL Injection Vulnerability	BigAntSoft BigAnt Office Messenger	✓	✗	✗

Vulnerability Details

#1

A critical zero-day vulnerability, CVE-2025-0364 has been identified in BigAnt Server, an enterprise instant messaging solution. This flaw allows unauthenticated remote attackers to execute arbitrary PHP code, leading to full system compromise.

#2

The vulnerability was uncovered during an investigation into CVE-2024-54761. Initially, CVE-2024-54761 was misclassified due to incorrect assumptions regarding privilege requirements. However, further analysis revealed additional insecure programming practices, which ultimately led to the discovery of CVE-2025-0364. This chain of events highlights how interconnected vulnerabilities can provide insights into broader security issues within a system.

#3 The issue stems from a weakness in the default SaaS registration mechanism, allowing attackers to create admin accounts simply by solving a CAPTCHA. Once admin access is gained, they can exploit the "Cloud Storage Addin" feature to upload and execute malicious PHP scripts, fully compromising the system.

#4 The impact is severe, as attackers can exfiltrate data, modify system settings, deploy additional exploits, and pivot to other systems within the network. The availability of public proof-of-concept exploits further elevates the risk, making it imperative for organizations using BigAnt Server to reassess their security posture immediately.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-0364	BigAnt Server 5.6.06 and below	cpe:2.3:a:bigantsoft:bigant_server:*:*:*:*:*:*:*	CWE-288
CVE-2024-54761	BigAnt Server 5.6.06 and below	cpe:2.3:a:bigantsoft:bigant_server:*:*:*:*:*:*:*	CWE-89

Recommendations

Disable the SaaS Registration Feature: Since the vulnerability exploits the default SaaS registration process, temporarily disable this feature to prevent unauthorized administrative account creation.

Restrict Access to the Cloud Storage Addin: Limit access to the “Cloud Storage Addin” by enforcing network segmentation or firewall rules. Only allow trusted internal users to access this feature.

Implement Additional Authentication Controls: Consider adding multi-factor authentication (MFA) or other supplementary authentication mechanisms to enhance account security, reducing the risk of unauthorized access.

Monitor Server Logs: Increase logging and monitoring to detect unusual activity such as unexpected administrative account creations or anomalous file uploads. This helps in early detection of any exploitation attempts.

Prepare for Immediate Patch Deployment: Once the latest patch version is released, plan for a swift upgrade to minimize exposure. Test the update in a staging environment before full deployment.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	T1078 Valid Accounts
T1059 Command and Scripting Interpreter	T1588 Obtain Capabilities	T1588.005 Exploits	T1190 Exploit Public-Facing Application
T1588.006 Vulnerabilities			

Patch Details

No official patch details are available yet, mitigate vulnerabilities by disabling SaaS registration until patches are released.

Link:
https://www.bigantsoft.com/download.html

References

https://securityonline.info/cve-2025-0364-cvss-9-8-bigant-server-zero-day-public-exploit-confirmed/

https://thesecmaster.com/blog/how-to-fix-cve-2025-0364-protect-bigantsoft-bigant-server-from-critical-unauthent

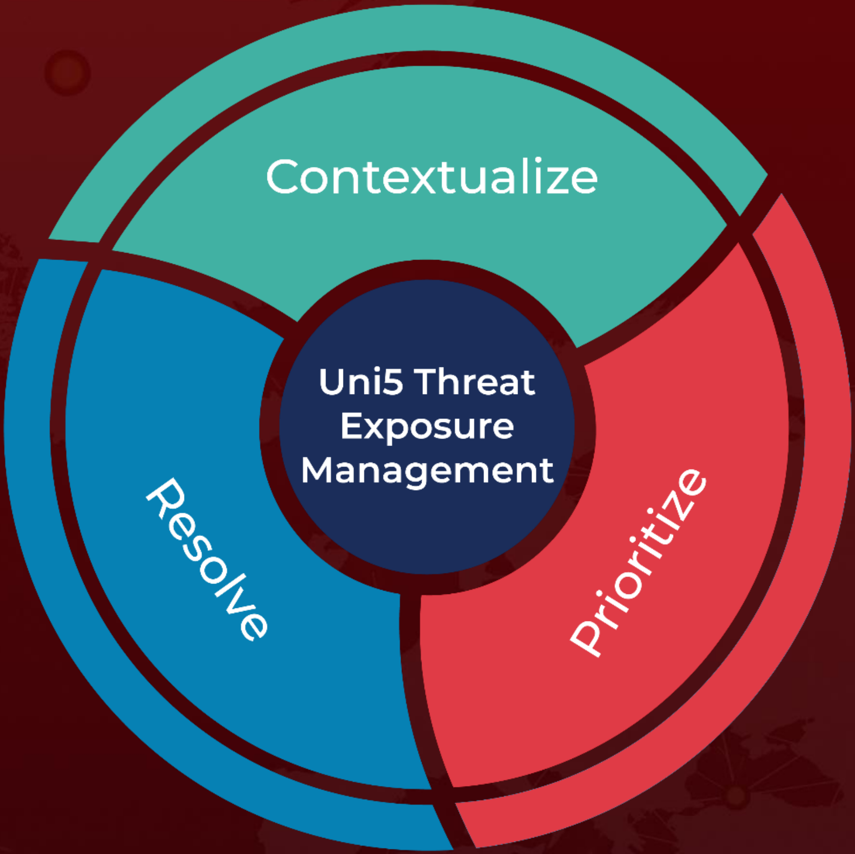
https://github.com/vulncheck-oss/cve-2025-0364

https://github.com/nscan9/CVE-2024-54761-BigAnt-Office-Messenger-5.6.06-RCE-via-SQL-Injection

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 5, 2025 • 4:30 AM

More at www.hivepro.com