VULNERABILITY BULLETINS

Patches Released for High-Severity Vulnerabilities Affecting Progress LoadMaster

TLP:WHITE

Feb 12, 2025

Progress Software recently addressed multiple high-severity vulnerabilities affecting its LoadMaster software. Successful exploitation of these vulnerabilities allows threat actors to execute malicious commands and exfiltrate system files.

Health-ISAC provides this information to increase situational awareness and encourages users to upgrade affected Progress LoadMaster versions.

The Progress LoadMaster solution is a high-performance application delivery controller (ADC) and load balancer software that manages and distributes traffic. The capabilities offered by the solution ensure the performance of business-critical applications and websites.

The security flaws affecting the application are a set of improper validation flaws and an improper input validation vulnerability. The improper input validation flaws, tracked as CVE-2024-56131, CVE-2024-56132, CVE-2024-56133, and CVE-2024-56135, allow threat actors that have successfully authenticated after gaining access to the management interface of LoadMaster to execute malicious commands via specially crafted HTTP requests.

Conversely, the improper validation vulnerability is tracked as CVE-2024-56134. The security flaw allows successfully authenticated

threat actors to access the management interface to download file contents available on the system through HTTP requests.

The vulnerabilities impact the following software versions:

- LoadMaster versions from 7.2.55.0 to 7.2.60.1 (inclusive) - Fixed in 7.2.61.0 (GA)
- LoadMaster versions from 7.2.49.0 to 7.2.54.12 (inclusive) - Fixed in 7.2.54.13 (LTSF)
- LoadMaster version 7.2.48.12 and prior - Upgrade to LTSF or GA
- Multi-Tenant LoadMaster version 7.1.35.12 and prior - Fixed in 7.1.35.13 (GA)

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to these vulnerabilities and take the necessary actions to ensure appropriate security measures are implemented, including:

- Applying the latest patches
- Sanitizing user inputs
- Blocking domain requests
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	HHS, The Hacker News, GB Hackers, Progress

Alert ID 5d9f210b

View Alert

Share Feedback

was this helpful? |

Tags CVE-2024-56135, CVE-2024-56134, CVE-2024-56133, CVE-2024-56132, CVE-2024-56131, Progress LoadMaster

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**