CYBER ADVISORY

TLP:CLEAR
09 SEP 2024

LoadMaster Security Vulnerability

LoadMaster | CVE-2024-7591 | Remote Code Execution | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a vulnerability known as CVE-2024-7591 with a reported CVSS V3.1 score of 10.0. The vulnerability affects LoadMaster 7.2.60.0, LoadMaster Multi-Tenant Hypervisor 7.1.35.11 and all prior versions for both software. Exploitation of this critical vulnerability could provide an attacker remote code execution (RCE) by access LoadMaster's management interface using a specially crafted HTTP request.[1][2]

Affected Product		Issues	CVE Identifier(s)	CVSS v3.1 score
LoadMaster Version 7.2.60.0 and all prior versions	**Multi-Tenant Hypervisor 7.1.35.11 and all prior versions**	Improper Input Validation vulnerability in Progress LoadMaster allows OS Command Injection.	CVE-2024-7591	10.0 Critical

Table 1: Vulnerable LoadMaster Products[3]

The Cal-CSIC recommends immediately upgrading all affected LoadMaster and Multi-Tenant Hypervisor to the Patched Version.

For further information on upgrading affected LoadMaster products, please refer to LoadMaster | Patched Version.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] Bleeping Computer; "Progress LoadMaster vulnerable to 10/10 severity RCE flaw;" https://www.bleepingcomputer.com/news/security/progress-loadmaster-vulnerable-to-10-10-severity-rce-flaw/; accessed 09 September 2024
[2] CVE Record; "CVE-2024-7591;" https://www.cve.org/CVERecord?id=CVE-2024-7591; accessed 09 September 2024
[3] Progress Kemp; "LoadMaster Security Vulnerability CVE-2024-7591;" https://support.kemptechnologies.com/hc/en-us/articles/29196371689613-LoadMaster-Security-Vulnerability-CVE-2024-7591; accessed 09 September 2024