Confidential

Cyber Threats

Monthly Cyber Intelligence Summary

September 2024

Mishcon de Reya

It’s business. But it’s personal.

September 2024 - Cyber Threat Update

Summary

Incident	Threat	Key points
Cryptocurrency companies targeted by North Korean social engineering attacks	Best practices include identity verification on different platforms, avoiding storing sensitive crypto data on internet-connected devices, and using multi-factor authentication.	If affected, actions include investigation, employing Incident Response playbooks, seeking legal advice, and potentially reporting to the NCSC and sharing information through the UK's CISP.
Software firm, Progress issues security fix for a critical vulnerability	The exploitation of LoadMaster hypervisors can lead to remote execution of commands by the attackers potentially allowing system disruption, data infiltration and malware infections.	Install the add-ons provided by Progress for the vulnerable versions, monitor network traffic for HTTP requests which is a common attack vector.

Preparing decision makers

Our monthly report prepares cybersecurity practitioners to make better tactical, operational and strategic decisions. We have distilled analysis of key events from the previous month which have learning points that can be actioned to improve security.

1. The document has three main purposes to assist cybersecurity leaders:
2. To be 'threat-led' and help prioritise defences against particular types of attackers
3. To justify business decisions on cybersecurity changes, technology or services

To enable them to respond confidently to questions from business leadership, defend decisions or make a case to change the status quo.

Cryptocurrency companies targeted by social engineering attacks.

What happened?

On 3rd September 2024, the US Federal Bureau of Investigation (FBI) issued an alert[1] that the Democratic People's Republic of Korea (DPRK), also known as North Korea, was actively engaging in sophisticated social engineering attacks targeting the cryptocurrency industry, particularly decentralised finance (DeFi) businesses. These attacks were aimed at deploying malware and stealing cryptocurrency by conducting extensive research on potential targets and crafting personalised fake scenarios to gain the trust of employees and access company networks. It is estimated that over $3Bn has been lost in similar attacks since 2017.[2]

North Korean actors have been observed researching companies associated with cryptocurrency exchange-traded funds (ETFs) and other financial products related to cryptocurrency, indicating a potential threat of cyber activities against these entities. The FBI has identified various tactics used by these actors, including impersonation, fluent English communication, and technical knowledge in the cryptocurrency field to build rapport and deliver malware.

So what?

The implications of these targeted attacks are significant for companies in the cryptocurrency sector, or those that handle cryptocurrency transactions. North Korea's persistent and advanced social engineering tactics pose a serious threat to organisations with substantial cryptocurrency assets. The FBI has provided a list of potential indicators of the activity, such as:

- unexpected employment offers from prominent firms
- requests to download applications or execute code; and
- insistence on using non-standard software for simple tasks.

There are several best practice guidance points to mitigate risks including verifying contacts' identities through separate communication platforms, not storing sensitive cryptocurrency information on internet-connected devices and using virtual machines for pre-employment tests involving code execution. Companies are also advised to implement multi-factor authentication, limit access to sensitive information, and use closed communication platforms with strict authentication protocols.

In the event of a severe social engineering attack, we advise rapid investigations, employing the appropriate Incident Response (IR) playbooks and engaging a specialist IR advisory team, including seeking legal advice around possible recovery of losses. We may also advise considering your obligations under data protection laws and reporting the incident to the National Cyber Security Centre (NCSC) in the UK.[3] These steps can help you recover, mitigate losses and remain compliant with regulatory and legal requirements. We may also advise that steps are taken to share intelligence through groups such as the UK's Cyber Security Information Sharing Partnership (CISP) to aid other investigations and learning.[4]

[1] North Korea Aggressively Targeting Crypto Industry with Well-Disguised Social Engineering Attacks, https://www.ic3.gov/Media/Y2024/PSA240903
[2] North Korean Hackers Stole $600 Million in Crypto in 2023, https://www.trmlabs.com/post/north-korean-hackers-stole-600-million-in-crypto-in-2023
[3] Report a Cyber Incident, https://report.ncsc.gov.uk/
[4] Apply for a CISP account, https://cispregistration.cisp.org.uk/

Software firm Progress issues a fix for a maximum severity vulnerability

What happened?

On 4th September 2024 software firm Progress issued a fix for a severe vulnerability impacting its LoadMaster Multi-Tenant (MT) and LoadMaster hypervisor products that allowed attackers to remotely execute commands on the device. [5]

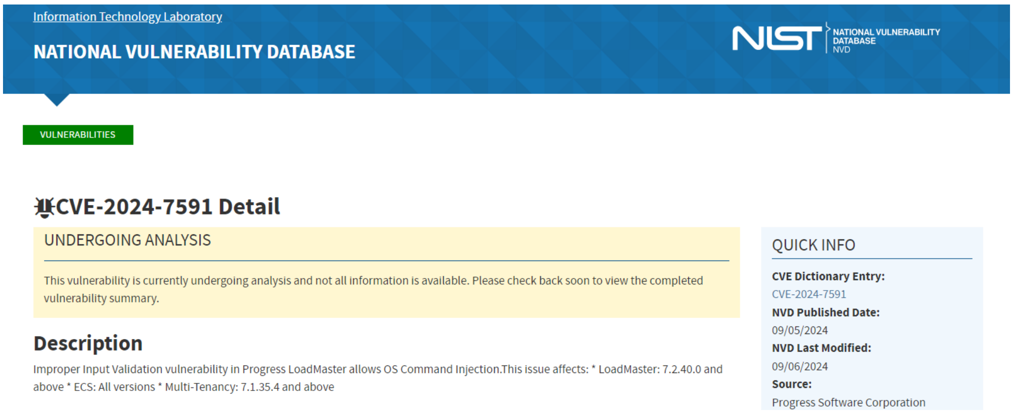
LoadMaster is an application delivery controller (ADC), a network component that helps distribute and manage traffic that comes to a website or web application, making sure the server does not get overwhelmed. The MT hypervisor allows independent running of applications while they share the same hardware platform.[6]

The vulnerability tracked as, CVE-2024-7591 has the highest score of 10 on the Common Vulnerability Score System (CVSS). Exploitation can potentially lead to the attacker gaining complete control over the affected system, leading to unauthorised access to confidential information, data exfiltration, service disruption, malware spread and significant reputational, financial and legal consequences for the affected organisation.

The vulnerability has been known to impact LoadMaster 7.2.60.0 and the MT Hypervisor 7.1.35.11 and all prior releases.[7]

Th flaw arises due to inadequate input validation mechanisms within the LoadMaster's management interface. This deficiency permits external actors to construct and dispatch specially crafted HTTP requests that can manipulate the system into executing unauthorised commands, effectively bypassing authentication protocols.

As per the updates on the CVE from NIST, as of 13 September, the vulnerability was undergoing analysis and we recommend continuous follow up until further details are revealed, as the National Vulnerability Database (NVD) offers references for further information, lists of affected software, and the dates of publication and last modification.


Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NIST NATIONAL VULNERABILITY DATABASE NVD
VULNERABILITIES

CVE-2024-7591 Detail

UNDERGOING ANALYSIS

This vulnerability is currently undergoing analysis and not all information is available. Please check back soon to view the completed vulnerability summary.

Description

Improper Input Validation vulnerability in Progress LoadMaster allows OS Command Injection.This issue affects: * LoadMaster: 7.2.40.0 and above * ECS: All versions * Multi-Tenancy: 7.1.35.4 and above

QUICK INFO

CVE Dictionary Entry:
CVE-2024-7591
NVD Published Date:
09/05/2024
NVD Last Modified:
09/06/2024
Source:
Progress Software Corporation

Figure 1: Updates on the vulnerability show it was still undergoing analysis (source: NIST)

[5] Progress LoadMaster vulnerable to 10/10 severity RCE flaw, https://www.bleepingcomputer.com/news/security/progress-loadmaster-vulnerable-to-10-10-severity-rce-flaw/

[6] Progress Software Issues Patch for Vulnerability in LoadMaster and MT Hypervisor, https://thehackernews.com/2024/09/progress-software-issues-patch-for.html

[7] Progress Software issues fix for maximum severity vulnerability, https://www.securitymagazine.com/articles/101030-progress-software-issues-fix-for-maximum-severity-vulnerability

So what?

Progress Software has developed an add-on package that can be installed on any of the vulnerable versions to mitigate the risk. This patch is crucial as it sanitises user input to prevent the execution of arbitrary system commands. It is important to note that the free version of LoadMaster does not receive this patch, leaving it susceptible to CVE-2024-7591.[8]

While there have been no reports of active exploitation, the potential severity of this vulnerability means that all users of the affected LoadMaster products should take immediate action to secure their systems. The recommended steps include:

— **Install the add-on**: Apply the emergency add-on package provided by Progress Software to all vulnerable versions of LoadMaster and LoadMaster MT Hypervisor.

— **Security hardening**: Follow the vendor's recommended security hardening measures to further protect the management interface from unauthorized access.

— **Monitor network traffic**: Keep an eye on network traffic for any unusual activity that could indicate an attempt to exploit this vulnerability, such as incoming HTTP request.

— **Access control**: Ensure that the management interface of LoadMaster is not accessible from untrusted networks. Use firewalls or other network security tools to restrict access.

Hypervisor products are targeted by cybercriminals because they often offer a high level of control over multiple virtual machines, access to a wide range of data, and opportunities for persistent and stealthy attacks. For these reasons it is prudent to exercise a heightened level of monitoring around these products.

By taking these proactive measures, organisations can defend against potential attacks that may seek to exploit this vulnerability and maintain the integrity and availability of their network services.[9]

[8] LoadMaster Security Vulnerability CVE-2024-7591, https://support.kemptechnologies.com/hc/en-us/articles/29196371689613-LoadMaster-Security-Vulnerability-CVE-2024-7591

[9] Technical Note LoadMaster Hardening, https://docs.progress.com/bundle/loadmaster-technical-note-loadmaster-hardening-ga/page/Introduction.html

Mishcon de Reya LLP
Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com

mishcon.com/cyber-risk-and-complex-investigations

The Traffic Light Protocol (TLP) is a set of designations used to ensure that senstive information is shared with the appropriate audience.

This document is marked TLP:GREEN meaning recipients may share with peers and partner organizations within their sector or community, but not via publicly accessible channels.

This document has been prepared for general guidance only and does not constitute professional or legal advice. If you wish to receive legal advice, we will need to provide you with a separate retainer letter and additional terms of business, as such work will be separately regulated by the Solicitors Regulation Authority (SRA).

You should not act upon the information contained in this publication without obtaining specific professional or legal advice.

Mishcon de Reya refers to Mishcon de Reya LLP, which is a limited liability partnership, incorporated in England (number OC399969), whose registered office is at Africa House, 70 Kingsway, London WC2B 6AH. It is a body corporate which has members rather than Partners.