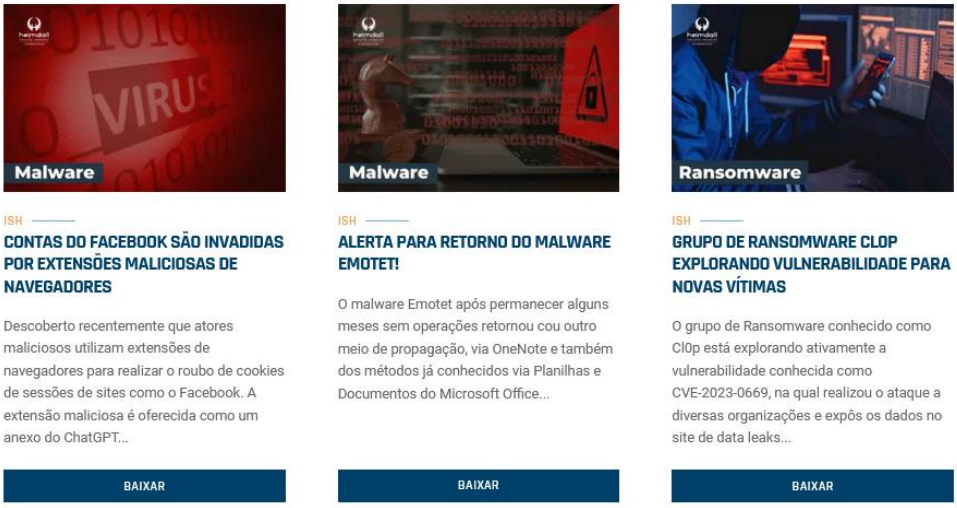
BOLETIM DE SEGURANÇA

Progress LoadMaster vulnerável a falha RCE de gravidade máxima

heimdall
security research
A DIVISION OF ISH

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



Sumário

1 Sumário Executivo 4
2 Produtos e versões afetadas 5
3 Recomendações 6
4 Referências 7
5 Autores 8

1 SUMÁRIO EXECUTIVO

A Progress Software disponibilizou uma correção emergencial para uma vulnerabilidade **crítica** (**pontuação de 10/10**) que afeta os produtos **LoadMaster** e **LoadMaster Multi-Tenant (MT) Hypervisor**, permitindo a execução remota de comandos nos dispositivos impactados. Identificada como **CVE-2024-7591**, a falha está relacionada a uma validação inadequada de entradas, permitindo que invasores não autenticados acessem a interface de gerenciamento do LoadMaster por meio de uma solicitação HTTP malformada.

2 PRODUTOS E VERSÕES AFETADAS

A falta de higienização da entrada do usuário também pode permitir que o invasor execute comandos arbitrários do sistema em endpoints vulneráveis. "É possível que invasores remotos não autenticados, com acesso à interface de gerenciamento do LoadMaster, enviem uma requisição HTTP cuidadosamente construída, permitindo a execução de comandos arbitrários no sistema", afirma o boletim de segurança da Progress.

Abaixo segue os produtos e versões afetadas pela falha:

- **LoadMaster:** 7.2.60.0 e todas as versões anteriores
- **Multi-Tenant Hypervisor:** 7.1.35.11 e todas as versões anteriores

Devido a explorações anteriores de falhas de segurança em produtos Progress por atores maliciosos, esta vulnerabilidade requer uma notável atenção.

3 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

- Instalação dos arquivos de validação XML disponibilizados na página de suporte.

Baixe o complemento pelos links disponíveis na página de suporte e instale-o utilizando os controles fornecidos na página ***System Configuration*** > ***System Administration*** > ***Update Software*** UI page.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Support.kemptechnologies
- Bleepingcomputer

5 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH