TLP: CLEAR

BOLETIM DE SEGURANÇA

Vulnerabilidade CVE-2025-0994 é explorada no Trimble Cityworks para execução remota de código

heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

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

Boletins de Segurança – Heimdall

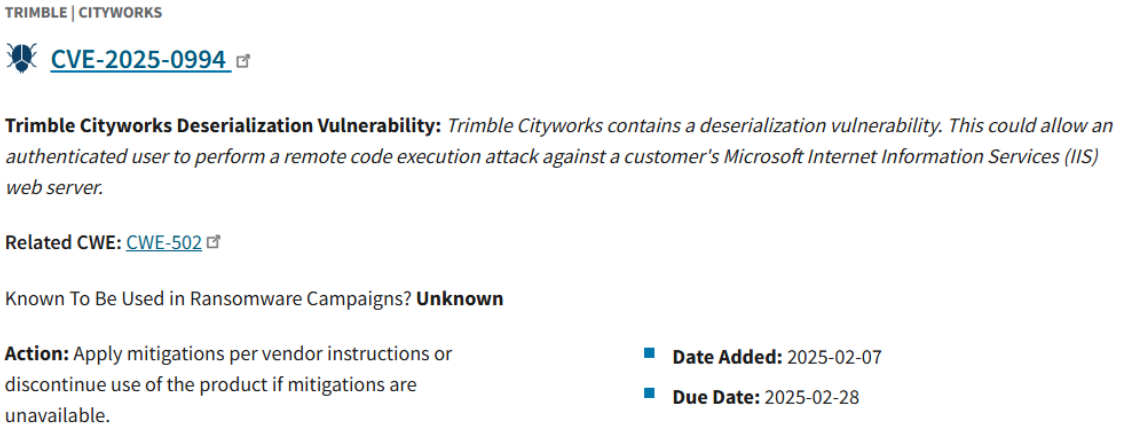
heimdall
security research
A DIVISION OF ISH

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

Uma vulnerabilidade grave identificada como CVE-2025-0994 foi descoberta no software Trimble Cityworks, permitindo que usuários autenticados realizem execução remota de código (RCE) em servidores Microsoft IIS. O Cityworks é amplamente utilizado por governos e serviços públicos, o que amplia o impacto potencial da falha. A vulnerabilidade está sendo ativamente explorada por hackers, que implantam ferramentas como o Cobalt Strike para obter acesso inicial às redes. A CISA e a Microsoft emitiram alertas devido ao risco elevado associado a essa exploração.



TRIMBLE | CITYWORKS

CVE-2025-0994

Trimble Cityworks Deserialization Vulnerability: *Trimble Cityworks contains a deserialization vulnerability. This could allow an authenticated user to perform a remote code execution attack against a customer's Microsoft Internet Information Services (IIS) web server.*

Related CWE: CWE-502

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-02-07
- **Due Date:** 2025-02-28

Figura 1 – Vulnerabilidade CVE-2025-0994 adicionada no catalogo KEV-CISA.

2 INFORMAÇÕES SOBRE A VULNERABILIDADE

A CVE-2025-0994 é uma vulnerabilidade de desserialização insegura que afeta o software Trimble Cityworks. Esta falha permite que usuários autenticados executem código remotamente (RCE) em servidores Microsoft IIS, potencialmente comprometendo a integridade das redes afetadas. A exploração bem-sucedida desta vulnerabilidade pode levar à instalação de malware, como o Cobalt Strike, e outras atividades maliciosas sem o conhecimento do usuário.

2.1 SISTEMAS E PRODUTOS AFETADOS

Abaixo segue os produtos e versões afetadas pela falha:

- *Trimble Cityworks versões anteriores à 15.8.9*
- *Trimble Cityworks with Office Companion versões anteriores à 23.10*

2.2 IMPACTO DA VULNERABILIDADE

A exploração da falha permite que atacantes autenticados executem código remotamente nos servidores afetados, resultando em:

- *Comprometimento da rede e acesso inicial não autorizado*
- *Instalação de malware, incluindo Cobalt Strike.*
- *Acesso não autorizado a dados sensíveis e sistemas internos*
- *Interrupção de serviços críticos e operações*

3 RECOMENDAÇÕES

Atualização imediata

- Atualize o Trimble Cityworks para a versão 15.8.9 e o Cityworks with Office Companion para a versão 23.10, que corrigem a vulnerabilidade CVE-2025-0994. As atualizações devem ser aplicadas imediatamente em todas as implantações locais.

Revisão de permissões do IIS

- Verifique e ajuste as permissões das identidades de aplicativos no Microsoft IIS, garantindo que não estejam configuradas com privilégios administrativos locais ou de nível de domínio, reduzindo o impacto de uma possível exploração.

Correção de configurações de diretórios

- Audite as configurações de diretório do Cityworks, garantindo que as pastas raiz de anexos contenham apenas os arquivos necessários e estejam devidamente protegidas contra acessos não autorizados.

Fortalecimento da segurança da rede

- Adote práticas adicionais de segurança, como segmentação de rede para isolar sistemas críticos, e implemente autenticação multifator (MFA) para dificultar o acesso não autorizado, mesmo em caso de exploração da vulnerabilidade.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CISA**
- **Bleepingcomputer**

5 AUTORES

- **Wesley Murat**

heimdall
security research
A DIVISION OF ISH