A CISA dos EUA adiciona falhas da Oracle, Mozilla, Microsoft Windows, Li

Data: 2025-10-07 07:04:25

Autor: Inteligência Against Invaders

A CISA dos EUA adiciona falhas da Oracle, Mozilla, Microsoft Windows, Linux Kernel e MicrosoftIE ao seu catálogo de vulnerabilidades exploradas conhecidas

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) adiciona falhas Oracle, Mozilla, Linux Kernel, Microsoft Windows e MicrosoftIE ao seu catálogo de Vulnerabilidades Exploradas Conhecidas.

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA)Adicionado Oracle, Linux Kernel, Mozilla, Microsoft Windows e MicrosoftIE falhas em seu Catálogo de vulnerabilidades exploradas conhecidas (KEV).

Abaixo estão as descrições dessas falhas:

- CVE-2010-3765Vulnerabilidade de execução remota de código de vários produtos da Mozilla
- CVE-2010-3962Vulnerabilidade de corrupção de memória não inicializada do Microsoft Internet Explorer
- CVE-2011-3402Vulnerabilidade de execução remota de código do Microsoft Windows
- CVE-2013-3918Vulnerabilidade de gravação fora dos limites do Microsoft Windows
- CVE-2021-22555Vulnerabilidade de gravação fora dos limites do heap do kernel do Linux
- CVE-2021-43226Vulnerabilidade de escalonamento de privilégios do Microsoft Windows
- CVE-2025-61882Vulnerabilidade não especificada do Oracle E-Business Suite

Esta semana, a Oracle Lançado um patch de emergência para resolver a vulnerabilidade crítica CVE-2025-61882 (CVSS 9.8) em seu E-Business Suite. A falha foi explorada peloCl0p ransomware grupo em ataques de roubo de dados. Invasores remotos não autenticados podem explorar a falha para assumir o controle do componente Oracle Concurrent Processing. O CVE-2025-61882 afeta o Oracle E-Business Suite 12.2.3–12.2.14 (BI Publisher Integration), especialistas alertam que é facilmente explorável via HTTP.

Algumas das falhas adicionadas ao catálogo KeV da CISA são muito apenas, como a falha CVE-2013-3918.

A vulnerabilidade CVE-2013-3918 foi originalmente usado pelo grupo APT por trás do 2009 Ataque Auroramas. em 2015 Kaspersky revelado que o ator do Estado-nação Grupo EQUAÇÃO capturou sua façanha e a reaproveitou para atingir usuários do governo no Afeganistão.

De acordo comDiretiva Operacional Vinculativa (BOD) 22-01: Reduzindo o Risco Significativo de Vulnerabilidades Exploradas Conhecidas, as agências FCEB precisam resolver as vulnerabilidades identificadas até a data de vencimento para proteger suas redes contra ataques que exploram as falhas no catálogo.

Os especialistas também recomendam que as organizações privadas revisem oCatálogoe abordar as vulnerabilidades em sua infraestrutura.

A CISA ordena que as agências federais corrijam as vulnerabilidades até 27 de outubro de 2025.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,CISA)