A CISA dos EUA adiciona falhas Smartbedded Meteobridge, Samsung, Jun

Data: 2025-10-04 16:03:05

Autor: Inteligência Against Invaders

A CISA dos EUA adiciona falhas Smartbedded Meteobridge, Samsung, Juniper ScreenOS, Jenkins e GNU Bash ao seu catálogo de vulnerabilidades exploradas conhecidas

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA) adiciona falhas Smartbedded Meteobridge, Samsung, Juniper ScreenOS, Jenkins e GNU Bash ao seu catálogo de vulnerabilidades exploradas conhecidas.

A Agência de Segurança Cibernética e Infraestrutura dos EUA (CISA)Adicionado Falhas inteligentes do Meteobridge, Samsung, Juniper ScreenOS, Jenkins e GNU Bash ao seu Catálogo de vulnerabilidades exploradas conhecidas (KEV).

Abaixo estão as descrições dessas falhas:

- CVE-2014-6278Vulnerabilidade de injeção de comando do GNU Bash OS
- CVE-2015-7755Vulnerabilidade de autenticação inadequada do Juniper ScreenOS
- CVE-2017-1000353Vulnerabilidade de execução remota de código do Jenkins
- CVE-2025-4008Vulnerabilidade de injeção de comando do Smartbedded Meteobridge
- CVE-2025-21043Vulnerabilidade de gravação fora dos limites de dispositivos móveis da Samsung

Em outubro de 2024, a comunidade de TI em todo o mundo ficou chocada com a descoberta doBash Bugfalha, uma vulnerabilidade que afetou o popular componente Bash por mais de duas décadas.

Enquanto os principais fornecedores trabalhavam para fornecer os patches necessários para sistemas Linux e Unix vulneráveis, o pesquisador Michal Zalewskiencontrou dois bugs adicionais no Bourne Again Shell.

Um dos dois bugs, rastreado comoCVE-2014-6278, como o original Vulnerabilidade de bug do Bash (CVE-2014-6271) pode ser explorado para execução remota de código arbitrário. Os especialistas explicaram que ele existe devido a uma correção incompleta para CVE-2014-6271, CVE-2014-7169 e CVE-2014-6277.

A segunda falha adicionada ao catálogo KeV, rastreada como CVE-2015-7755, em um problema de acesso administrativo. Os invasores remotos podem explorar a falha para obter acesso administrativo digitando uma senha não especificada durante uma sessão (1) SSH ou (2) TELNET.

A terceira edição adicionada ao catálogo, rastreada como CVE-2017-1000353, é uma vulnerabilidade de execução remota de código não autenticada que permitia que invasores transferissem um objeto Java SignedObject serializado para a CLI Jenkins baseada em comunicação remota, que seria desserializada usando um novo ObjectInputStream, ignorando o mecanismo de proteção baseado em lista negra existente.

SignedObject foi adicionado à lista negra de comunicação remota." lê oConsultoria de segurança publicado por Jenkins.

A CISA também adicionou a vulnerabilidade CVE-2025-4008 ao catálogo. O problema é uma falha de injeção de comando na interface da web do Smartbedded MeteoBridge que permite que invasores remotos e não autenticados executem comandos root arbitrários.

O último problema adicionado ao catálogo afeta os dispositivos Samsung, é uma gravação fora dos limites rastreada como CVE-2025-21043. A vulnerabilidade reside no libimagecodec.quram.so anterior ao SMR Sep-2025 Release 1. Um invasor remoto pode explorar a falha para executar código arbitrário.

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 23 de outubro de 2025.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,CISA)