TLP: CLEAR

BOLETIM DE SEGURANÇA

Vulnerabilidades no SAP NetWeaver permitem acesso não autorizado ao sistema

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

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO EXECUTIVA

A SAP divulgou em seu Portal de Suporte duas vulnerabilidades críticas no **SAP NetWeaver Application Server** para ABAP e na **Plataforma ABAP**, designadas como **CVE-2025-0070** e **CVE-2025-0066**. Essas falhas podem permitir que atacantes obtenham acesso não autorizado a sistemas SAP, comprometendo a confidencialidade, integridade e disponibilidade das aplicações afetadas.

Figura 1 – Mapa de calor de dispositivos SAP NetWeaver Application Server expostos na Internet-Fofa.info.

Conforme ilustrado na imagem acima, é possível identificar milhares de dispositivos ***SAP NetWeaver Application Server*** expostos na Internet. Embora muitas organizações configurem esses servidores para acesso restrito dentro de redes privadas, diversas circunstâncias podem levar à sua exposição pública, seja de forma intencional ou acidental. Essa exposição representa um risco significativo de segurança, especialmente para organizações suscetíveis às vulnerabilidades abordadas neste relatório.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

A vulnerabilidade CVE-2025-0070 é classificada como uma falha de autenticação inadequada (CWE-287). Ela permite que um invasor autenticado explore fraquezas nos mecanismos de autenticação do SAP NetWeaver Application Server para ABAP e na Plataforma ABAP. A exploração pode levar ao escalonamento de privilégios, permitindo que o invasor acesse dados sensíveis, manipule configurações e interrompa operações do sistema. O ataque pode ser realizado remotamente via rede, com baixa complexidade e sem necessidade de interação do usuário, tornando-o relativamente fácil de ser explorado.

A falha CVE-2025-0066 decorre de controles de acesso inadequados no Internet Communication Framework do SAP NetWeaver AS para ABAP e na Plataforma ABAP (CWE-732). Sob certas condições, permite que invasores acessem informações restritas, potencialmente comprometendo a confidencialidade, integridade e disponibilidade das aplicações afetadas. Semelhante à **CVE-2025-0070**, este ataque pode ser realizado remotamente com baixa complexidade e requer privilégios mínimos.

2.1 SISTEMAS E PRODUTOS AFETADOS

Abaixo segue os produtos e versões afetadas pelas falhas:

CVE-2025-0070

- SAP NetWeaver Application Server para ABAP, versões *KRNL64NUC 7.22, 7.53, 8.04*, até *9.14*.
- Plataforma ABAP, versões *KRNL64NUC 7.22, 7.53, 8.04*, até *9.14*.

CVE-2025-0066

- SAP NetWeaver AS para ABAP, versões *SAP_BASIS 700* até *SAP_BASIS 914*.
- Plataforma ABAP, versões *SAP_BASIS 700* até *SAP_BASIS 914*.

2.2 IMPACTO DAS VULNERABILIDADES

A exploração bem-sucedida dessas vulnerabilidades pode acarretar graves consequências para o ambiente afetado, resultando em:

- Escalonamento de privilégios.
- Manipulação de configurações e potencial interrupção das operações do sistema.
- Acesso não autorizado a informações restritas.

3 RECOMENDAÇÕES

Aplicar patches

- Aplicar todas as atualizações de segurança disponíveis fornecidas pela SAP.

Revisar e fortalecer controles de acesso

- Implementar controles de acesso rigorosos e revisar permissões existentes para garantir que apenas usuários autorizados tenham acesso a dados e funcionalidades sensíveis.

Monitorar tentativas de autenticação

- Estabelecer monitoramento contínuo para detectar e responder a tentativas de autenticação suspeitas ou falhas.

Segregar redes

- Utilizar segmentação de rede para isolar sistemas críticos e minimizar o potencial de movimentação lateral por parte de atacantes.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **SAP**
- **CVE**
- **CWE**
- **Cyber Security News**

5 AUTORES

- **Rafael Salomé**

heimdall
security research
A DIVISION OF ISH