BOLETIM DE SEGURANÇA

Identificada vulnerabilidade alta para produtos Adobe Acrobat e Reader

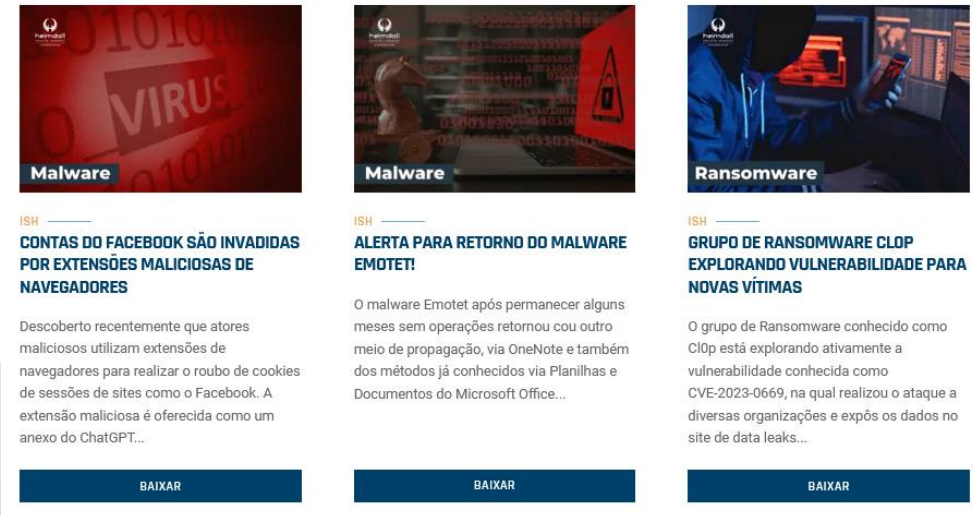
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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 Tabelas

1 SOBRE A VULNERABILIDADE

A Adobe publicou atualizações de segurança para corrigir uma vulnerabilidade de zero day no Acrobat e no Reader marcada como altamente explorada em ataques.

A vulnerabilidade foi catalogada como **CVE-2023-26369** e pode permitir que atores maliciosos obtenham a execução de código após explorarem com sucesso um ponto fraco na gravação fora dos limites. A base de pontuação da vulnerabilidade é de **8,8 (alta)**.

De acordo com a análise da vulnerabilidade, esta requer que o ator de ameaça esteja localmente na rede e requer interação do usuário.

Abaixo, estão os produtos e as versões afetadas:

Produto	Acompanhar	Versão afetada
Acrobat DC	Contínuo	23.003.20284 e anteriores
Acrobat Reader DC	Contínuo	23.003.20284 e anteriores
Acrobat 2020	Clássico 2020	20.005.30516 (Mac) e anteriores 20.005.30514 (Win) e anteriores
Acrobat Reader 2020	Clássico 2020	20.005.30516 (Mac) e anteriores 20.005.30514 (Win) e anteriores

Tabela 1 – Versões afetadas do Acrobat e Reader pela CVE-2023-26369.

Além da vulnerabilidade comentada acima, a Adobe corrigiu mais falhas de segurança que podem permitir que invasores obtenham a execução arbitrária de códigos em sistemas que executam o software Adobe Connect e Adobe Experience Manager.

Os bugs do Connect (CVE-2023-29305 e CVE-2023-29306) e do Experience Manager (CVE-2023-38214 e CVE-2023-38215) corrigidos hoje podem ser usados para lançar ataques refletidos de Cross-Site-Scripting (XSS).

Altamente recomendado que as organizações **acompanhem as atualizações, recomendando aplicarem as atualizações** de segurança para os softwares mencionados.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Publicação de comunicação da Adobe Reader e Acrobat**

heimdall
security research
A DIVISION OF ISH