BOLETIM DE SEGURANÇA

Falhas recentes no BIG-IP Next Central Manager possibilitam o controle total de dispositivos

heimdall
security research
A DIVISION OF ISH

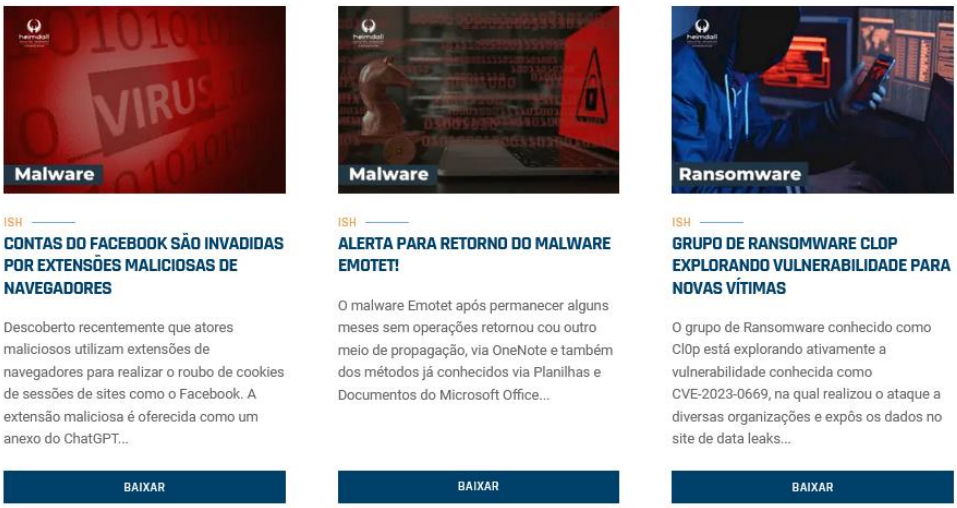
TLP: CLEAR

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

[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 SUMÁRIO EXECUTIVO

Recentemente duas falhas sérias no *BIG-IP Next Central Manager* foram corrigidas pela **F5**, as quais podem ser usadas para obter controle total e criar contas secretas não autorizadas em qualquer dispositivo gerenciado. Falha de injeção de SQL CVE-2024-26026 e outra de injeção de OData CVE-2024-21793 na API do BIG-IP Next Central Manager. Estas falhas possibilitam que invasores não autorizados executem instruções SQL maliciosas remotamente em dispositivos que ainda não foram corrigidos.

2 DETALHES SOBRE EXPLORAÇÃO DAS VULNERABILIDADES

A empresa de segurança Eclypsium revelou que, ao explorar falhas, descobriu uma maneira de criar contas fraudulentas sem deixar rastros no sistema de gerenciamento centralizado. Isso significa que, mesmo após invadir uma instância não corrigida, as contas criadas não seriam detectadas pelo Next Central Manager, permitindo assim que os invasores mantenham acesso malicioso sem serem notados. O console de gerenciamento pode ser acessado remotamente por meio de certas vulnerabilidades, concedendo controle total ao invasor sobre o gerenciador. Isso possibilita a exploração de outras vulnerabilidades para criar novas contas em dispositivos gerenciados, as quais não seriam visíveis no BIG-IP Next gerenciado pelo Central Manager.

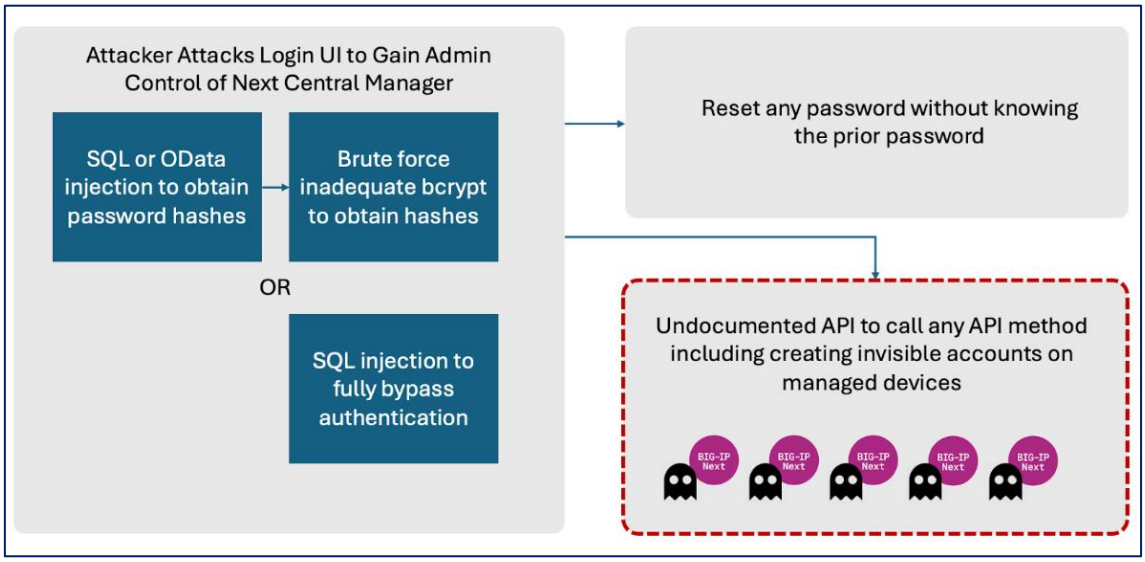


Figura 1 – Caminhos de ataques.

Segundo a BIG-IP o produto e versões afetados pelas falhas são:

- BIG-IP Next Central Manager - 20.0.1 - 20.1.0

3 DISPOSITIVOS BIG-IP EXPOSTOS ONLINE

Com uma busca por dispositivos BIG-IP em plataformas de inteligência, conforme demonstram as imagens abaixo, é possível observar uma grande variedade de dispositivos com portas de gerenciamento expostas online.

Figura 2 – Dispositivos expostos online-Shodan.io.

Figura 3 – Dispositivos expostos online-Fofa.info.

Mesmo o Brasil não estando como os países com mais dispositivos expostos online, ainda assim, isso, requer um devida atenção por parte dos administradores , devido a explorações de atores maliciosos nestes dispositivos.

4 RECOMENDAÇÕES

- Atualizar para versão recente 20.2.0
- Seguindo as diretrizes da F5, os administradores são aconselhados a restringir o acesso do Next Central Manager apenas a usuários confiáveis em uma rede segura, caso não possam aplicar as atualizações de segurança imediatamente. Isso visa reduzir os possíveis riscos de ataques.

Porém devido à alta utilização de dispositivos BIG-IP no Brasil e no mundo, e explorações por atores maliciosos sobre esses dispositivos, é aconselhado a atualização.

5 CONCLUSÃO

A utilização de dispositivos BIG-IP por atores maliciosos destaca uma área crítica de preocupação na segurança cibernética. Esses dispositivos, comumente usados para gerenciar tráfego de rede e garantir a disponibilidade e segurança de sistemas, tornam-se alvos atrativos devido ao seu papel central em infraestruturas de TI. Quando comprometidos, podem permitir o controle de fluxo de dados sensíveis, a implementação de ataques DDoS ou até mesmo a interceptação de informações confidenciais. Isso evidencia a importância das organizações implementarem estratégias robustas de segurança, monitoramento contínuo e atualizações regulares para proteger esses dispositivos de ameaças crescentes.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- F5-CVE-2024-26026
- F5-CVE-2024-21793
- Eclypsium
- Bleepingcomputer

7 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH