TLP: CLEAR

BOLETIM DE SEGURANÇA

5 vulnerabilidades divulgadas pela Fortinet consideradas Graves e Críticas

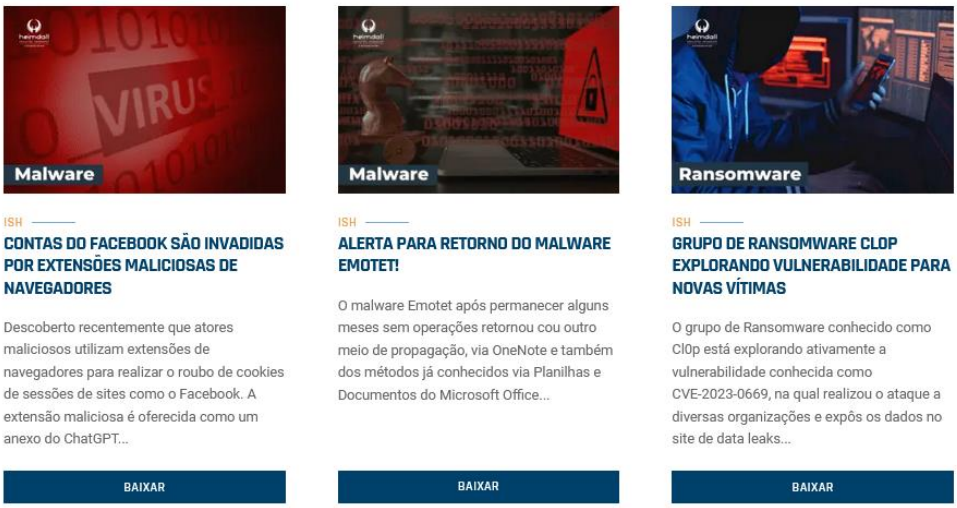
heimdall
security research
A DIVISION OF ISH

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 TABELAS

1 SOBRE AS VULNERABILIDADES

A **Fortinet** divulgou **5 novas vulnerabilidades** com classificações de gravidade "crítica" ou "alta" na terça-feira, levando a CISA a emitir um aviso.

As falhas afetam os produtos Fortinet, incluindo FortiClient EMS, FortiManager, FortiOS e FortiProxy, as quais foram detalhadas abaixo:

- **CVE-2023-47534**
- **FG-IR-23-390**

FortiClientEMS: Poderá causar a execução de códigos ou comandos não autorizados (RCE).

Gravidade: **Alta** com pontuação **8.7.**

Solução:

Versão	Afetados	Solução
FortiClientEMS 7.2	7.2.0 a 7.2.2	Atualize para 7.2.3 ou superior
FortiClientEMS 7.0	7.0.0 a 7.0.10	Atualize para 7.0.11 ou superior
FortiClientEMS 6.4	6.4 todas as versões	Migrar para uma versão fixa
FortiClientEMS 6.2	6.2 todas as versões	Migrar para uma versão fixa
FortiClientEMS 6.0	6.0 todas as versões	Migrar para uma versão fixa

Tabela 1 – Produtos afetados – CVE-2023-47534.

- **CVE-2023-42789 e CVE-2023-42790**
- **FG-IR-23-328**

FortiOS e FortiProxy: Poderá ocasionar a gravação fora dos limites no portal e um buffer overflow baseado em pilha, permitindo que um invasor interno que tenha acesso ao portal captive execute códigos ou comandos arbitrários via especialmente solicitações HTTP elaboradas.

Gravidade: **Crítica** com pontuação **9.3**.

Solução:

"Gambiarra": Definir um esquema de autenticação não baseado em formulário:

```
config authentication scheme
edit scheme
set method method
next
```

```
end
```

Onde o **<method>** pode ser qualquer um abaixo:

```
ntlm NTLM authentication.
basic Basic HTTP authentication.
digest Digest HTTP authentication.
negotiate Negotiate authentication.
fsso Fortinet Single Sign-On (FSSO) authentication.
rsso RADIUS Single Sign-On (RSSO) authentication.
ssh-publickey Public key based SSH authentication.
cert Client certificate authentication.
saml SAML authentication
```

Produtos:

Afetados	Soluções
FortiOS versão 7.4.0 a 7.4.1	Atualize para o FortiOS versão 7.4.2 ou superior
FortiOS versão 7.2.0 a 7.2.5	Atualize para o FortiOS versão 7.2.6 ou superior
FortiOS versão 7.0.0 a 7.0.12	Atualize para o FortiOS versão 7.0.13 ou superior
FortiOS versão 6.4.0 a 6.4.14	Atualize para o FortiOS versão 6.4.15 ou superior
FortiOS versão 6.2.0 a 6.2.15	Atualize para o FortiOS versão 6.2.16 ou superior
FortiProxy versão 7.4.0	Atualize para o FortiProxy versão 7.4.1 ou superior
FortiProxy versão 7.2.0 a 7.2.6	Atualize para o FortiProxy versão 7.2.7 ou superior
FortiProxy versão 7.0.0 a 7.0.12	Atualize para o FortiProxy versão 7.0.13 ou superior
FortiProxy versão 2.0.0 a 2.0.13	Atualize para o FortiProxy versão 2.0.14 ou superior
	A Fortinet no terceiro trimestre de 23 corrigiu esse problema no FortiSASE versão 23.3.b e, portanto, os clientes não precisam realizar nenhuma ação.

Tabela 2 – Produtos afetados – CVE-2023-42789 e CVE-2023-42790.

Um Patch virtual denominado **“FortiOS.Captive.Portal.Out.Of.Bounds.Write”** está disponível na atualização FMWP db 23.105

- **CVE-2024-23112**
- **FG-IR-24-013**

FortiOS e FortiProxy: Um desvio de autorização através da vulnerabilidade de chave controlada pelo usuário no FortiOS e FortiProxy SSLVPN pode permitir que um invasor autenticado obtenha acesso aos favoritos de outros usuários por meio da manipulação de URL.

Gravidade: **Alta** com pontuação **7.2**.

Solução:

“Gambiarra”: Desative o modo web SSL VPN.

Versão	Afetados	Solução
FortiOS 7.4	7.4.0 a 7.4.1	Atualize para 7.4.2 ou superior
FortiOS 7.2	7.2.0 a 7.2.6	Atualize para 7.2.7 ou superior
FortiOS 7.0	7.0.1 a 7.0.13	Atualize para 7.0.14 ou superior
FortiOS 6.4	6.4.7 a 6.4.14	Atualize para 6.4.15 ou superior
FortiProxy 7.4	7.4.0 a 7.4.2	Atualize para 7.4.3 ou superior
FortiProxy 7.2	7.2.0 a 7.2.8	Atualize para 7.2.9 ou superior
FortiProxy 7.0	7.0.0 a 7.0.14	Atualize para 7.0.15 ou superior

Tabela 3 – Produtos afetados – CVE-2024-23112.

- **CVE-2023-36554**
- **FG-IR-23-103**

FortiWLM MEA: Uma vulnerabilidade de controle de acesso impróprio no FortiWLM MEA para FortiManager pode permitir que um invasor remoto não autenticado execute códigos ou comandos arbitrários por meio de solicitações especificamente criadas.

O FortiWLM MEA não é instalado por padrão no FortiManager e pode ser desabitado como solução alternativa.

Gravidade: **Alta** com pontuação **7.7**.

Solução:

Afetados	Soluções
FortiManager versão 7.4.0	Atualize para o FortiManager versão 7.4.1 ou superior
FortiManager versão 7.2.0 a 7.2.3	Atualize para o FortiManager versão 7.2.4 ou superior
FortiManager versão 7.0.0 a 7.0.10	Atualize para o FortiManager versão 7.0.11 ou superior
FortiManager versão 6.4.0 a 6.4.13	Atualize para o FortiManager versão 6.4.14 ou superior
FortiManager 6.2 todas as versões	

Tabela 4 – Produtos afetados – CVE-2023-36554.

- **CVE-2023-48788**
- **FG-IR-24-007**

FortiClientEMS: Uma neutralização inadequada de elementos especiais usados em uma vulnerabilidade de comando SQL (SQL Injetion) no FortiClientEMS pode

permitir que um invasor não autenticado execute códigos ou comandos não autorizados por meio de solicitações especificamente criadas.

Gravidade: **Crítica** com pontuação **9.3**.

Solução:

Versão	Afetados	Solução
FortiClientEMS 7.2	7.2.0 a 7.2.2	Atualize para 7.2.3 ou superior
FortiClientEMS 7.0	7.0.1 a 7.0.10	Atualize para 7.0.11 ou superior

Tabela 5 – Produtos afetados – CVE-2023-48788.

2 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**

heimdall
security research
A DIVISION OF ISH