TLP: CLEAR

BOLETIM DE SEGURANÇA

CISA emite alerta para exploração ativa de vulnerabilidades no Zyxel, ProjectSend e CyberPanel

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.

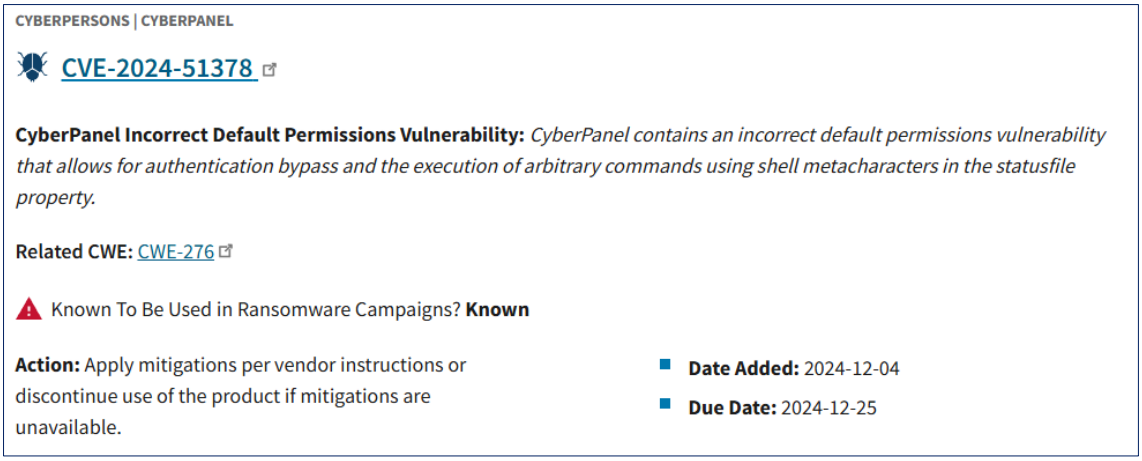
Boletins de Segurança – Heimdall

SUMÁRIO

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

A **Agência de Segurança Cibernética e de Infraestrutura dos EUA (CISA**) incluiu no seu catálogo de **Vulnerabilidades Exploradas Conhecidas (KEV)** novas falhas de segurança identificadas em produtos da **Zyxel**, **North Grid Proself**, **ProjectSend** e **CyberPanel**, destacando que essas vulnerabilidades estão sendo exploradas ativamente.


CYBERPERSONS | CYBERPANEL

CVE-2024-51378

CyberPanel Incorrect Default Permissions Vulnerability: *CyberPanel contains an incorrect default permissions vulnerability that allows for authentication bypass and the execution of arbitrary commands using shell metacharacters in the statusfile property.*

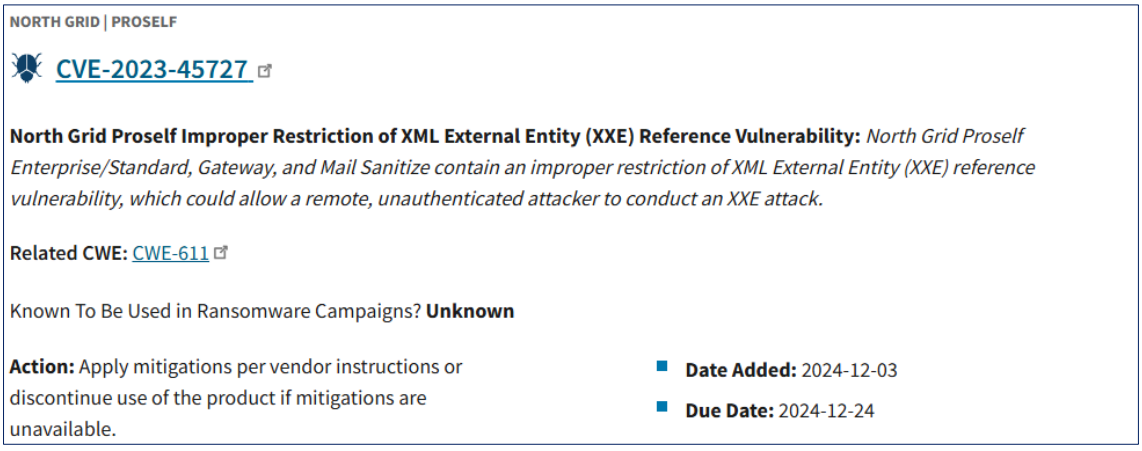
Related CWE: CWE-276

Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-12-04
- **Due Date:** 2024-12-25

Figura 1 – Vulnerabilidade CVE-2024-51378 no Catálogo KEV-CISA.


NORTH GRID | PROSELF

CVE-2023-45727

North Grid Proself Improper Restriction of XML External Entity (XXE) Reference Vulnerability: *North Grid Proself Enterprise/Standard, Gateway, and Mail Sanitize contain an improper restriction of XML External Entity (XXE) reference vulnerability, which could allow a remote, unauthenticated attacker to conduct an XXE attack.*

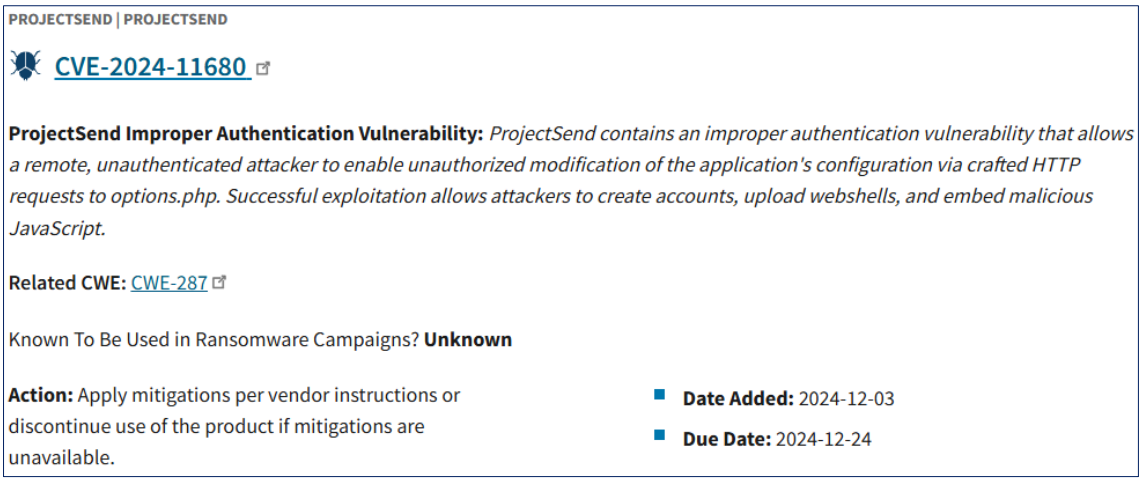
Related CWE: CWE-611

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-12-03
- **Due Date:** 2024-12-24

Figura 2 – Vulnerabilidade CVE-2023-45727 no Catálogo KEV-CISA.


PROJECTSEND | PROJECTSEND

CVE-2024-11680

ProjectSend Improper Authentication Vulnerability: *ProjectSend contains an improper authentication vulnerability that allows a remote, unauthenticated attacker to enable unauthorized modification of the application's configuration via crafted HTTP requests to options.php. Successful exploitation allows attackers to create accounts, upload webshells, and embed malicious JavaScript.*

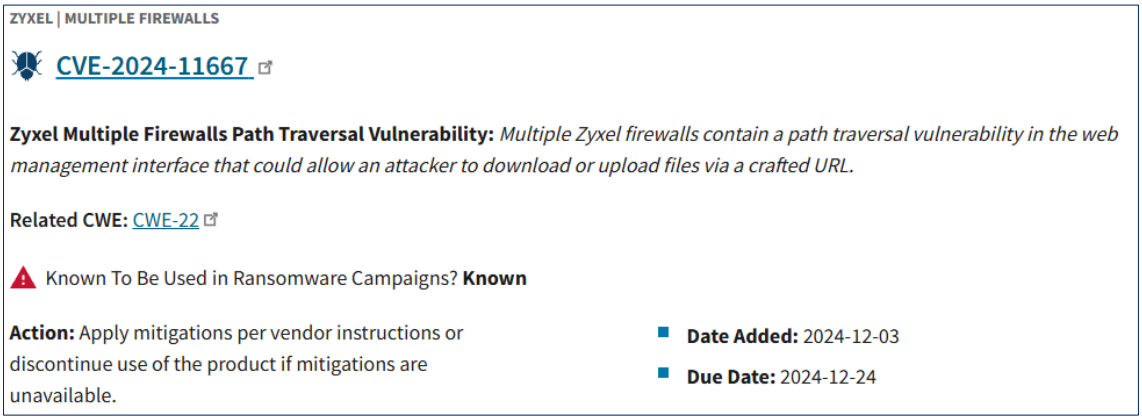
Related CWE: CWE-287

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-12-03
- **Due Date:** 2024-12-24

Figura 3 – Vulnerabilidade CVE-2024-11680 no Catálogo KEV-CISA.


ZYXEL | MULTIPLE FIREWALLS

CVE-2024-11667

Zyxel Multiple Firewalls Path Traversal Vulnerability: *Multiple Zyxel firewalls contain a path traversal vulnerability in the web management interface that could allow an attacker to download or upload files via a crafted URL.*

Related CWE: CWE-22

Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-12-03
- **Due Date:** 2024-12-24

Figura 4 – Vulnerabilidade CVE-2024-11667 no Catálogo KEV-CISA.

2 INFORMAÇÕES SOBRE AS VULNERABILIDADES

Segue a lista de vulnerabilidades informadas pela CISA, juntamente com uma breve descrição de cada uma:

CVE-2024-51378

O **CyberPanel** contém uma falha nas permissões padrão que possibilita o desvio de autenticação e a execução de comandos arbitrários utilizando **metacaracteres** de shell na propriedade *statusfile*.

CVE-2023-45727

O **North Grid Proself Enterprise/Standard, Gateway Mail Sanitize** contêm uma vulnerabilidade relacionada à restrição inadequada de referências de Entidade Externa XML (XXE), que pode permitir a realização de ataques XXE por um invasor remoto e não autenticado. Essa vulnerabilidade foi adicionada ao catálogo KEV após a publicação de um relatório da Trend Micro, em novembro de 2024, que associou sua exploração ativa a um grupo de espionagem cibernética ligado à China, conhecido como **Earth Kasha**, também chamado de MirrorFace.

CVE-2024-11680

O **ProjectSend** contém ma falha de autenticação inadequada que possibilita a **criação de contas**, upload de *web shells* e inserção de JavaScript malicioso por um invasor remoto e não autenticado. O fornecedor de segurança cibernética VulnCheck revelou recentemente que agentes mal-intencionados começaram a explorar essa vulnerabilidade em setembro de 2024, com o objetivo de utilizá-la para implantar cargas úteis pós-exploração.

CVE-2024-11667

Firewalls **Zyxel** contêm uma vulnerabilidade de **travessia de diretórios** na interface de gerenciamento da web, permitindo que um invasor carregue ou baixe arquivos utilizando uma URL manipulada.

3 RECOMENDAÇÕES

Recomendamos fortemente que as organizações minimizem sua exposição a ataques cibernéticos, dando prioridade à rápida **correção das vulnerabilidades** como parte essencial de suas práticas de gestão de riscos e vulnerabilidades.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **NVD**
- **CISA**
- **The Hacker News**

5 AUTORES

- **Rafael de Moura Salomé**

heimdall
security research
A DIVISION OF ISH