



CNCS



Centro Nacional
de Cibersegurança
PORTUGAL

Classificação de Incidentes

TAXONOMIA

CENTRO NACIONAL DE CIBERSEGURANÇA

Classificação de Incidentes

Taxonomia

O CERT.PT utiliza para a sua classificação de incidentes a taxonomia da Rede Nacional de CSIRT, discriminada na tabela abaixo.

Classe Incidente	Tipo Incidente
Código Malicioso	Sistema Infetado
	Distribuição de Malware
	Servidor C2
	Configuração de Malware
Disponibilidade	Negação de Serviço
	Negação de Serviço Distribuída
	Configuração incorreta
	Sabotagem
	Interrupção
Recolha de Informação	Scanning
	Sniffing
	Engenharia Social
Intrusão	Comprometimento de Conta Privilegiada
	Comprometimento de Conta Não Privilegiada
	Comprometimento de Aplicação
	Comprometimento de Sistema
	Arrombamento

Classe Incidente	Tipo Incidente
Tentativa de Intrusão	Exploração de Vulnerabilidade
	Tentativa de Login
	Nova assinatura de ataque
Segurança da Informação	Acesso não autorizado
	Modificação não autorizada
	Perda de dados
	Exfiltração de Informação
Fraude	Utilização indevida ou não autorizada de recursos
	Direitos de autor
	Utilização ilegítima de nome de terceiros
	Phishing
Conteúdo Abusivo	SPAM
	Discurso Nocivo
	Exploração sexual de menores, racismo e apologia da violência
Vulnerabilidade	Criptografia fraca
	Amplificador DDoS
	Serviços acessíveis potencialmente indesejados
	Revelação de informação
	Sistema vulnerável
Outro	Sem tipo
	Indeterminado

Para mais detalhes/informação acerca da Taxonomia em vigor existe um documento disponível no website da RNCSIRT, disponível no seguinte URL:
https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf