Zona de Alertas e Notícias de Cibersegurança

O que precisa de saber, em resumo

Esta é uma área de consulta com informação atualizada sobre vulnerabilidades técnicas e incidentes de cibersegurança com impacto relevante — para que cidadãos, empresas e entidades públicas saibam, de forma simples, quando algo exige a sua atenção.

O QUE VAI ENCONTRAR

ALERTAS DE VULNERABILIDADE	NOTÍCIAS DE INCIDENTES SIGNIFICATIVOS
Falhas de segurança conhecidas em sistemas, aplicações e serviços — com indicação do produto afetado e da gravidade.	Casos reais de ciberataques com impacto relevante, em Portugal e no estrangeiro, e as lições que deles se podem retirar.

Alertas de Vulnerabilidades - Modelo do cartão (a preencher):

DD MÊS AAAA	Alerta de Vulnerabilidade – [Produto / Fabricante]	
TIPO Vulnerabilidade	**SISTEMAS AFETADOS** [Sistema(s) e versão(ões) afetados]	**ECOSSISTEMA** [Fabricante / Outro]
CRITICIDADE (CVSS) [Ex.: 9,8 — Crítica]	**ESTADO** [Ativo / Mitigado / Corrigido]	**FONTE** [Link para o aviso original]

Notícias de incidentes significativos - Modelo do cartão (a preencher):

DD MÊS AAAA	[Título sintético do incidente]	
SETOR / ENTIDADE AFETADA **[Setor / entidade afetada]**	**TIPO DE INCIDENTE** **[Ex.: Ransomware, Fuga de dados, DDoS, Supply chain]**	**FONTE** **[Fonte / link]**
RESUMO DO IMPACTO **[Síntese factual do incidente, impacto conhecido e, quando aplicável, relevância para o perfil de risco da organização. Exemplo ilustrativo — a substituir por conteúdo real no momento da publicação.]**		

PORQUE É QUE ISTO LHE DIZ RESPEITO

Cidadão	Alerta para quando atualizar aplicações e serviços que usa no dia a dia — telemóvel, computador, aplicações bancárias, redes sociais.
Empresas	Identificação atempada de vulnerabilidades no software que utiliza, para priorizar correções antes de serem exploradas por atacantes.
Entidades da Administração Pública Regional e Local	Apoio ao dever de vigilância tecnológica no âmbito do Regime Jurídico da Cibersegurança (NIS2) e critério de referência para a avaliação de risco.

O QUE DEVE FAZER

- Consultar regularmente e verificar se algum alerta afeta sistemas ou aplicações que utiliza.
- Aplicar as atualizações de segurança recomendadas pelo fabricante assim que disponíveis.
- Entidades abrangidas pelo RJC/NIS2: em caso de incidente confirmado, notificar o CNCS através da plataforma MyCiber.

ONDE CONSULTAR MAIS

Fonte	Ligação	Para que serve
CNCS — Alertas	https://dyn.cncs.gov.pt/pt/alertas	Alertas oficiais de vulnerabilidades para Portugal — fonte de referência desta página.
ENISA — Base de Dados Europeia de Vulnerabilidades	https://euvd.enisa.europa.eu/	Vulnerabilidades a nível europeu, com contexto adicional.
CVE.org (CVE Program / MITRE)	https://www.cve.org/	Registo oficial e autoritário dos identificadores CVE.
NVD — National Vulnerability Database (NIST)	https://nvd.nist.gov/vuln/search	Base de dados de vulnerabilidades do NIST (EUA); enriquece cada CVE com pontuação CVSS e metadados técnicos.
CISA — Known Exploited Vulnerabilities Catalog	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	Catálogo de vulnerabilidades com exploração ativa confirmada; critério de priorização definido na secção 1.2.