Veröffentlicht auf Presseportal Schweiz - Presse und Medienmitteilungen (https://www.presseportal-schweiz.ch)

17.10. 2022

Kritische Fortinet-Schwachstelle: 533 direkt angreifbare IT-Systeme in der Schweiz identifiziert

Von Dreamlab Techn...

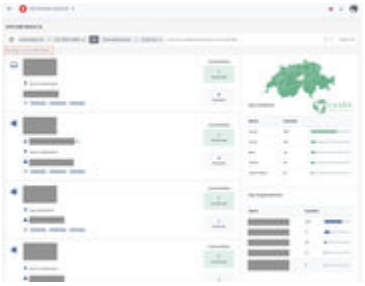

Bild Rechte
Dreamlab Technologies AG

(Bern)(PPS) **Die seit zehn Tagen bekannte kritische Fortinet-Schwachstelle CVE-2022-40684 erlaubt Hackern, sich mit Administratorenrechten in verwundbare Systeme einzuloggen. Aktuellste Messungen legen offen, dass die IT-Infrastrukturen von 533 Schweizer Unternehmen diesbezüglich weiterhin ungeschützt sind. Unter den angreifbaren Firmen befinden sich mehrere Telekommunikationsanbieter, ISPs und Elektrizitätswerke. Schnelles Handeln ist dringend notwendig.**

Fortinet warnte am 6. und am 10. Oktober 2022 davor, dass die dokumentierte Schwachstelle CVE-2022-40684 "Critical Authentication Bypass“ ihre drei Produkte FortiOS, FortiProxy und FortiSwitchManager betrifft. Die Schwachstelle hat mit 9.6 einen hohen CVSS-Score (Common Vulnerability Scoring System) und ermöglicht Angreifenden, sich mit Administratorenrechten in das betroffene System einzuloggen. Am 13. Oktober 2022 wurde von Horizon3-Forschern gezeigt, wie die Schwachstelle ausgenutzt werden kann.

Am 15. Oktober 2022 identifizierte das von Dreamlab Technologies entwickelte Cyberradarsystem «CyObs» 533 ungeschützte Fortinet-Geräte in der Schweiz (siehe Abbildung). CyObs führt regelmässig wissenschaftliche Scans der Schweizer Internet-Infrastruktur durch und gleicht die Resultate mit der CVE-Datenbank ab (Common Vulnerabilities and Exposures).

Da die kriminelle Ausnutzung der Schwachstelle zu grossen Schäden führen kann, informiert Dreamlab Technologies am 17. Oktober 2022 sämtliche 533 betroffenen Unternehmen in der Schweiz direkt.

Zu den betroffenen Schweizer Unternehmen gehören mehrere Telekommunikationsanbieter, ISPs, Elektrizitätswerke und Produktionsfirmen. Dreamlab Technologies legt den betroffenen Unternehmen dringend nahe, ihre Fortinet-Infrastrukturen so rasch als möglich zu patchen. Es gibt Grund anzunehmen, dass sich kriminelle Organisationen in den nächsten Tagen auf Schweizer Infrastrukturen mit dieser Schwachstelle fokussieren werden.

Informationen von Fortinet zur kritischen Schwachstelle werden hier publiziert: https://www.fortinet.com/blog/psirt-blogs/update-regarding-cve-2022-406….

Zum CyObs Cyberradarsystem

CyObs ist ein von Dreamlab Technologies entwickeltes hochpräzises Cyberradarsystem, welches Angriffsflächen im digitalen Raum nachweisbar minimiert. CyObs beinhaltet die lückenlose Abdeckung des Cyberraums inklusive Abhängigkeiten und Schnittstellen, zuverlässige Diagnosen mit Empfehlungen in Echtzeit, systematische Analysen von Cyberangriffen sowie vollautomatische Scans, ergänzt durch präzise Messungen.

Weitere Informationen zu CyObs: https://cyobs.com/

Über die Organisation:

Zu Dreamlab Technologies AG
Dreamlab Technologies ist ein führendes Schweizer IT-Sicherheitsunternehmen mit Standorten auf vier Kontinenten. Die Kombination von technischem Fachwissen und ausgewiesener internationaler Expertise ermöglicht es Dreamlab, Cybersicherheit auf der Grundlage quantifizierbarer und verifizierbarer Open-Standard-Technologien zu

entwickeln, zu bewerten und zu kontrollieren. Dreamlab berät Staaten, Organisationen und Behörden und hilft ihnen, das Bewusstsein für Informationssicherheit in ihren Managementzyklus zu entwickeln und integrieren. Nebst den Softwareprodukten CyObs, CySOC und vielen weiteren Lösungen bietet Dreamlab an allen Standorten hochqualifizierte IT-Sicherheitsaudits und Schulungen an.

Weitere Informationen: https://dreamlab.net/

Pressekontakt:

Dreamlab Technologies AG
Monbijoustrasse 36
3011 Bern, Schweiz

www.dreamlab.net

Nicolas Mayencourt, CEO
+41 79 757 97 25
nicolas.mayencourt @ dreamlab.net

Prof. Dr. Marc K. Peter, COO
+41 79 300 55 60
marc.peter @ dreamlab.net

Kategorie
IT & Software & Neue Medien
