CISA warnt: Kritische Citrix-Sicherheitslücke gefährdet Behörden!

CISA warnt vor aktiver Ausnutzung der Sicherheitslücke "CitrixBleed-2". Unternehmen sollten dringend Patches anwenden.

United States - In der Cybersecurity-Welt gibt es derzeit ein Thema, das für ordentlich Aufregung sorgt: die CitrixBleed-2-Lücke. Die US-amerikanische Cybersecurity- und Infrastruktur-Sicherheitsbehörde CISA hat diese kritische Sicherheitsanfälligkeit nun in ihren Katalog der ȝKnown Exploited Vulnerabilitiesȝ (KEV) aufgenommen, was Unternehmen alles andere als kalt lassen sollte. Gemäß einer Meldung von all-about-security.de wird die Schwachstelle, die auch als CVE-2025-5777 klassifiziert ist, aktiv ausgenutzt und stellt somit ein erhebliches Risiko dar.

Betroffen sind vor allem Nutzer der Produkte Citrix NetScaler ADC und Gateway, die einen Lesezugriff außerhalb des

zulässigen Bereichs ermöglichen. CISA hat Betreiber neuerdings aufgefordert, umgehend Sicherheitsmaßnahmen zu ergreifen. Dies ist besonders dringend, da diese Art von Sicherheitslücken häufig als Angriffsvektoren dienen, gerade für Bundesbehörden, die besonders schützenswert sind.

Dringlichkeit der Maßnahmen

Besonders alarmierend ist, dass CISA eine Frist von nur einem Tag für Bundesbehörden gesetzt hat, um Patches anzuwenden – eine Vorgabe, die als beispiellos angesehen wird. Laut bleepingcomputer.com wurde die Sicherheitsanfälligkeit bereits am 10. Juni 2025 in den Katalog aufgenommen, und seitdem haben Sicherheitsforscher konstant vor ihrer Schwere gewarnt. Es handelt sich um eine kritische Speicheranfälligkeit, die unbefugten Zugriff auf geschützte Bereiche ermöglicht. Daher ist schnelles Handeln gefragt!

Die betroffenen Versionen von NetScaler sind alle darauf angewiesen, rechtzeitig auf die neuesten Builds zu aktualisieren, um Neuangriffe abzuwehren. Von den neuen Firmware-Updates profitieren die Versionen 14.1-43.56+, 13.1-58.32+ und 13.1-FIPS/NDcPP 13.1-37.235+. Nutzer sollten auch an die Trennung aktiver Sitzungen denken, um mögliche Kompromittierungen zu vermeiden.

Die Softwareanpassungen und Sicherheitssysteme

Am 17. Juni 2025 veröffentlichte Citrix diese Updates, jedoch hat es bis heute einige Verwirrung über den Status der Ausnutzung gegeben, da eine ursprüngliche Sicherheitsmitteilung von Citrix vom 27. Juni 2025, die auf kein aktives Ausnutzen in der Wildnis hinwies, nicht aktualisiert wurde. Selbst nach der Warnung von Sicherheitsforscher Kevin Beaumont über die Ernsthaftigkeit der Situation am 24. Juni blieb der Druck auf die betroffenen Unternehmen hoch, da Bedrohungsakteure aktiv in Hackerforen

über die Probleme diskutierten.

Für Unternehmen, die Gewissheit hinsichtlich ihrer Cybersecurity-Strategie suchen, bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) wertvolle Informationen und Empfehlungen. Die BSI-Webseite bietet zahlreiche Hinweise zur Verbesserung der Cybersicherheit für alle Arten von Unternehmen. Hier finden Sie Informationen zu Prävention, Reaktion und Detektion, die für Unternehmen unerlässlich sind, um sich gegen aktuelle Cyberrisiken abzusichern.

In dieser schnelllebigen Digitalisierung sind Schwachstellen wie die CitrixBleed-2-Lücke ständige Begleiter. Wir empfehlen jedem, der mit den betroffenen Systemen arbeitet, die Sicherheitsrichtlinien einzuhalten und proaktiv zu handeln, denn wie man so schön sagt: Wo der Rauch ist, da steckt oft auch das Feuer!

All-about-security.de berichtet, dass die CitrixBleed-2-Lücke aktiv ausgenutzt wird, während bleepingcomputer.com die Dringlichkeit von schnellen Fixes unterstreicht. Mehr Informationen zu sicherheitsrelevanten Themen erhalten Sie außerdem beim BSI.

Details	
Ort	United States
Quellen	• www.all-about-security.de • www.bleepingcomputer.com • www.bsi.bund.de