AZ:

Der Landesbeauftragte für Datenschutz MV sieht dringenden Handlungsbedarf - Sicherheitslücke „React2Shell“ in weit verbreiteter Webtechnologie

Derzeit besteht eine gravierende Schwachstelle (CVE-2025-66478 und CVE-2025-55182) in den so genannten React Server Components (RSC), die weit verbreitet für die Entwicklung von Webseiten und Webanwendungen eingesetzt werden.

Die bekannt gewordene Schwachstelle kann dazu führen, dass Angreifende Schadcode einschleusen oder unbefugt auf Inhalte von Webanwendungen zugreifen. Damit besteht auch das Risiko, dass personenbezogene Daten kompromittiert werden.

Die Schwachstelle, die bereits am 3. Dezember öffentlich gemacht wurde, wird inzwischen weltweit massiv ausgenutzt und es gibt Schätzungen zufolge allein in Deutschland ca. 15.000 betroffene Webanwendungen. Verantwortliche sind infolgedessen angehalten, umgehend zu prüfen, ob sie von dieser Sicherheitslücke betroffen sind. Die empfohlenen Sicherheitsupdates bzw. Konfigurationen müssen daher unverzüglich angewendet werden. Zudem sollten die Verantwortlichen ihre Webserver und Webanwendungen eingehend auf eine bereits erfolgte Kompromittierung prüfen, insbesondere dann, wenn nicht zeitnah nach Bekanntwerden der Schwachstelle notwendige Maßnahmen ergriffen wurden oder andere technische Maßnahmen eine Kompromittierung verhindern konnten. Es ist davon auszugehen, dass eine Kompromittierung der Webanwendung bzw. des Webservers wahrscheinlich ist, sofern nicht umgehend gehandelt wurde.

Wichtig ist in diesem Zusammenhang nochmal darauf hinzuweisen, dass Verantwortliche einen Überblick darüber haben sollten, welche Komponenten, also welche Pakete und Bibliotheken, in der Software ihrer Anwendungen und Systeme eingesetzt werden, bekannt auch als „Software Bill of Materials“. Nur so kann sichergestellt werden, dass rechtzeitig und zielgerichtet auf regelmäßig auftretende Sicherheitslücken reagiert werden kann.

„Werden bekannte Sicherheitslücken ausgenutzt, kann das für Verantwortliche schnell teuer werden, wenn diese nicht versucht haben sie umgehend zu schließen oder sie gar leichtfertig ermöglicht wurden. Neben den unmittelbaren Kosten, die aus einem solchen Datenabfluss resultieren können, drohen auch Schadenersatzansprüche aus der DSGVO.“ warnt Mecklenburg-Vorpommerns Landesdatenschutzbeauftragter Sebastian Schmidt. Passiert doch etwas, rät er dringend zur Meldung an die zuständige Datenschutzaufsichtsbehörde. „Wer nicht meldet, riskiert im schlimmsten Fall sogar ein Bußgeld.“

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt generell den Einsatz einer Web Application Firewall (WAF) in Umgebungen mit erhöhtem Schutzbedarf und hat im IT-Grundschutz weitere Maßnahmen veröffentlicht, um Webanwendungen und Webserver generell abzusichern.

Weitere Infos:

AZ:

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2025/2025-304569-1032.html

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_3_1_Webanwendungen_und_Webservices_Edition_2023

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_3_2_Webserver_Edition_2023