

A part of **Department of Communications, Climate Action & Environment**

---



## **NCSC Flash Advisory**

---

Critical Vulnerability in SAP NetWeaver AS Java (CVE-2020-6287)  
2020-07-14

Status: **TLP-WHITE**

<b>Threat Type</b>	<p>On July 13, SAP released a security update to address a critical vulnerability, CVE-2020-6287, affecting the SAP NetWeaver Application Server (AS) Java component LM Configuration Wizard. An unauthenticated attacker can exploit this vulnerability through the Hypertext Transfer Protocol (HTTP) to take control of trusted SAP applications.</p> <p>The NCSC advises all constituents to apply the updates immediately as directed by <a href="#">SAP</a>.</p>
<b>Products Affected</b>	<p>This vulnerability is present by default in SAP applications running on top of SAP NetWeaver AS Java 7.3 and any newer versions (up to SAP NetWeaver 7.5). Potentially vulnerable SAP business solutions include any SAP Java-based solutions.</p>
<b>Impact</b>	<p>If successfully exploited, a remote, unauthenticated attacker can obtain unrestricted access to SAP systems through the creation of high-privileged users and the execution of arbitrary operating system commands with the privileges of the SAP service user account (&lt;sid&gt;adm), which has unrestricted access to the SAP database and is able to perform application maintenance activities, such as shutting down federated SAP applications.</p> <p>The confidentiality, integrity, and availability of the data and processes hosted by the SAP application are at risk by this vulnerability.</p>
<b>Recommendations</b>	<p>The NCSC advises affected users to ensure that the updates issued by SAP are applied as soon as possible, see <a href="https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675">https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675</a></p> <p>Organizations that are unable to immediately patch should mitigate the vulnerability by disabling the LM Configuration Wizard service. Should these options be unavailable or if the actions will take more than 24 hours to complete, NCSC strongly recommends closely monitoring your SAP NetWeaver AS for anomalous activity.</p>