National Cyber Security Centre

21090701001-NCSC

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

NCSC Alert

Confluence Server Webwork OGNL injection - CVE-2021-26084
2021-09-07

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Threat Type	The NCSC are aware of active exploitation of CVE-2021-26084 in Atlassian Confluence Server and Data Center systems. CVE-2021-26084 refers to an OGNL injection in the Confluence Server Webwork, that would allow unauthenticated users, to execute arbitary code on a Confluence Server or Data Center Instances. The Object-Graph Navigation Language (OGNL) is an open-source expression language for getting and setting properties of Java objects. The NCSC has observed mass exploitation of this vulnerability, such as deployment of crypto currency miners. Administrators should commence incident response procedures on their Confluence servers if still vulnerable, in order to assess if any compromise has occurred. **This vulnerability only affects on-premise servers, not those hosted in the cloud.**
Products Affected	**The following versions of Confluence server and Data Center instances.** • All 4.x.x versions - 7.12.x versions • All 6.13.x versions before 6.13.23 • All 7.4.x versions before 7.4.11 • All 7.11.x versions before 7.11.6 • All 7.12.x versions before 7.12.5
Impact	Remote Code Execution - compromised systems, data loss.
Recommendations	The NCSC recommends that affected organisations update Confluence server and Confluence Data Center instances as soon as possible. Upgrade to the latest Long Term Support release. For a full description of the latest version, see the Confluence Server and Data Center Release Notes. You can also download the latest version from their download centre. If you are running an affected version upgrade to version 7.13.0 (LTS) or higher. If you are running 6.13.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 6.13.23. If you are running 7.4.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.4.11. If you are running 7.11.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.11.6. If you are running 7.12.x versions and cannot upgrade to 7.13.0 (LTS) then upgrade to version 7.12.5.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie