National Cyber Security Centre

2206161221-NCSC

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

NCSC Alert

Vulnerabilities in Splunk Enterprise deployment servers (CVE-2022-32157) (CVE-2022-32158)
2022-06-16

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.*

Description

Splunk have published details related to vulnerabilities in Splunk Enterprise deployment servers.

CVE-2022-32158 (CVSSv3.1 9.0): Organisations running vulnerable instances of Splunk Enterprise deployment server, can allow clients to deploy forwarder bundles to other deployment clients through the deployment server. An attacker that compromises a Universal Forwarder endpoint could use this vulnerability to execute arbitary code on any Universal Forwarder endpoints subscribed to that deployment server. Please see Splunks announcement for more information on this vulnerability.

CVE-2022-32157 (CVSSv3.1 7.5): Organisations running vulnerable instances of Splunk Enterprise deployment server, can allow unauthenticated downloading of forwarder bundles. Please see Splunks announcement for more information on this vulnerability.

The Splunk Cloud Platform (SCP) is not affected by either of these vulnerabilities. At the time of writing, there is no evidence that these vulnerabilities are being actively exploited by threat actors in the wild.

Products Affected

- Splunk Enterprise running any version before 9.0.

Impact

Unauthenticated remote code execution - compromised systems, data loss.

Recommendations

The NCSC recommends that affected organisations upgrade Splunk Enterprise and Universal Forwarders to version 9.0 or higher. Once upgraded, authentication for deployment servers and clients must be configured in order to fully mitigate CVE-2022-32157. Once enabled, deployment servers can manage only Universal Forwarder versions 9.0 and later. Though the vulnerability does not directly affect Universal Forwarders, remediation requires updating all Universal Forwarders that the deployment server manages to version 9.0 or higher prior for the remediation to take effect.

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
LinkedIn: ncsc-ie