OneSpan Security Advisory

Remote code execution vulnerability in Apache Struts 2 component in OneSpan products

Advisory ID: onespan-sa-20180828-struts

Revision number: 1.1

Date and time of release: August 28 2018 17:00 UTC

Date and time of last update: August 31 2018 09:30 UTC

Summary

On 22 August 2018 the Apache Struts project issued a security bulletin about a Remote Code Execution vulnerability that exists in Apache Struts 2. This vulnerability is referred to as CVE-2018-11776. The vulnerability could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system.

This security advisory contains information on the OneSpan products that have been affected by the vulnerability and contains information on the availability of hotfixes.

Impacted products

Following OneSpan products are affected by the CVE-2018-11776 vulnerability:

- Authentication Server 3.8 and later
- Appliance 3.8.9.0 and later

Detailed description of vulnerability

The vulnerability exists in Apache Struts because the affected software insufficiently validates user-supplied input, allowing the use of results with no namespace value and the use of url tags with no value or action. In cases where upper actions or configurations also have no namespace or a wildcard namespace, an attacker could exploit this vulnerability by sending a request that submits malicious input to the affected application for processing. If successful, the attacker could execute arbitrary code in the security context of the affected application on the targeted system.

To exploit this vulnerability, an attacker must send a request that submits malicious input to the targeted system, making exploitation more difficult in environments that restrict network access from untrusted sources.

In scope of OneSpan's Authentication Server, Appliance and Virtual Appliance, the vulnerability is present in the web administration component. The vulnerability can only be exploited by a malicious user if this user has access to web resources of the web administration component, such as the login page of the web administration component.

Severity score

The table below denotes the CVSS 2.0 vulnerability score of the CVE-2018-11776 vulnerability in OneSpan's products.

CVSS Base Score: 6.8 (medium)					
Access Vector	**Access Complexity**	**Authentication**	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
Network	Medium	None	Partial	Partial	Partial

Product fixes and workarounds

OneSpan is releasing hotfixes for the following products:

- Authentication Server 3.8.2, 3.9.1, 3.10.1 R2, 3.11.1 R2, 3.12.2 R3, 3.13.1 R2, 3.14.1 R2, 3.15, 3.16
- Appliance 3.8.9.0, 3.8.9.1, 3.9.10.1, 3.9.10.0, 3.10.11.0, 3.11.12.1, 3.11.12.0, 3.12.13.0, 3.12.13.1, 3.13.14.0, 3.14.15.0

OneSpan is releasing patches for the following products: Appliance 3.16.

Hotfixes for Authentication Server are expected to be available by the end of the week of 27 August 2018. Hotfixes and patches for Appliance are expected to be available by the end of the week of 3 September 2018.

In order to limit the exploitability of the vulnerability, customers should limit the access to the web administration component as much as possible.

Obtaining product releases with fixes

Customers with a maintenance contract can obtain fixed product releases from the Customer Portal. Customers without a maintenance contract should contact their local sales representative.

References

[1] https://cwiki.apache.org/confluence/display/WW/S2-057
[2] https://nvd.nist.gov/vuln/detail/CVE-2018-11776

Legal disclaimer