Sehr geehrte Kundinnen und Kunden,

wir informieren Sie über mehrere kürzlich bekannt gewordenen Schwachstellen in Splunk Enterprise, Splunk Add-Ons, und den von Splunk mitgelieferten 3rd party libraries bei den Universal Forwardern. Hier wurden insbesondere Schwachstellen der Stufe hoch und auch kritisch behandelt, die zur Umgehung von Sicherheitsvorkehrungen im Produkt genutzt werden können, oder sogar Remotecode Ausführung ermöglichen.

Betroffene Lösungen:

- Splunk Universal Forwarder 9.0.0 bis 9.0.6
- Splunk Universal Forwarder 9.1.0 bis 9.1.1
- Splunk Web 9.0.0 bis 9.0.6 in Splunk Enterprise 9.0
- Splunk Web 9.1.0 bis 9.1.1 in Splunk Enterprise 9.1
- Splunk Web alle Versionen unterhalb von 9.1.2308 in Splunk Cloud
- Splunk Add-on für Google Cloud Plattform Versionen unterhalb von 4.3.0
- Splunk Add-on für Amazon Web Services Versionen unterhalb von 7.2.0

Infoquellen/Referenzen:
SPLUNK.com

Unsere empfohlenen Maßnahmen dazu:
Folgen Sie den Hinweisen des Herstellers und führen Sie die entsprechenden Upgrades durch. Damit werden auch noch weitere wichtige, nicht kritische oder hohe, Schwachstellen behoben.

Bei Fragen zu diesem Thema unterstützen wir Sie gerne unter **support@bacher.at** oder +43 60 126-34. Falls die erforderliche Maßnahme nicht durch Ihren Betriebsführungs- oder Support-Vertrag abgedeckt ist, bieten wir Ihnen auf Rückfrage gerne an, die Arbeiten durch unsere Spezialisten durchzuführen.

Mit freundlichen Grüßen

Ihr Bacher Support Team

Dear Customers,

Splunk recently informed about several vulnerabilities in Splunk Enterprise, Splunk Add-Ons and 3rd party libraries for Universal Forwarders. In particular, Splunk addressed high and critical rated vulnerabilities that can be used to circumvent security measures in the product or even enable remote code execution.

Affected solutions:

- Splunk Universal Forwarder 9.0.0 to 9.0.6
- Splunk Universal Forwarder 9.1.0 to 9.1.1
- Splunk Web 9.0.0 to 9.0.6 in Splunk Enterprise 9.0
- Splunk Web 9.1.0 to 9.1.1 in Splunk Enterprise 9.1
- Splunk Web all versions below 9.1.2308 in Splunk Cloud
- Splunk Add-on for Google Cloud Platform versions below 4.3.0
- Splunk Add-on for Amazon Web Services versions below 7.2.0

Sources/references:
SPLUNK.com

Our Recommendations:
Follow the given procedures from splunk and implement the upgrades accordingly. It also resolves further non-critical, but important vulnerabilities.

If you have any further questions, please do not hesitate to contact us at **support@bacher.at** or +43 1 60 126-34. In case this is not already covered by your operational contract we gladly offer to have this change implemented by one of our engineers on request.

Best regards

Bacher Systems Support Team