Sehr geehrte Kundinnen und Kunden,

wir informieren Sie über kürzlich veröffentlichte und als hoch eingestufte, Schwachstellen in splunk Enterprise Web und splunk ITSI. Unter bestimmten Voraussetzungen kann schadhafter Code ausgeführt oder Cross site scripting (XSS) ermöglicht werden.

Betroffene Lösungen:

- Splunk Enterprise 8.2.0 bis 8.2.11
- Splunk Enterprise 9.0.0 bis 9.0.5
- Splunk Enterprise 9.1.0
- Splunk Cloud **(ACHTUNG - das Patching der splunk Cloud Umgebung erfolgt durch den Hersteller selbst)**
- Splunk ITSI → 4.13.0 bis 4.13.2
- Splunk ITSI → 4.15.0 bis 4.15.2

Infoquellen/Referenzen:
SPLUNK.com

Unsere empfohlenen Maßnahmen dazu:
Folgen Sie den Hinweisen des Herstellers und führen Sie die Upgrades entsprechend Ihrer im Einsatz befindlichen Version durch. Splunk Enterprise Versionen 8.2.12, 9.0.6, und 9.1.1 bzw. splunk ITSI 4.13.3 und 4.15.3 beinhalten Patches für die diversen Schwachstellen. Es werden dabei auch noch weitere wichtige Schwachstellen behoben, die weniger problematisch eingestuft sind.

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,

we would like to inform you about recently released vulnerabilities rated with severity high in splunk Enterprise web and splunk ITSI. Under certain conditions attackers can execute arbitrary code or cross site scripting (XSS) could be allowed.

Affected solutions:

- Splunk Enterprise 8.2.0 to 8.2.11
- Splunk Enterprise 9.0.0 to 9.0.5
- Splunk Enterprise 9.1.0
- Splunk Cloud **(CAUTION - Splunk is actively upgrading Splunk Cloud deployments)**
- Splunk ITSI → 4.13.0 to 4.13.2
- Splunk ITSI → 4.15.0 to 4.15.2

Sources/references:
SPLUNK.com

Our Recommendations:
Follow the procedures from splunk and upgrade accordingly to your used software version. Splunk Enterprise versions 8.2.12, 9.0.6, and 9.1.1, as well as splunk ITSI 4.13.3 and 4.15.3 already include patches for the given vulnerabilities. In addition, several other important issues can be resolved by using these latest versions.

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