

Sehr geehrte Kundinnen und Kunden,

wir informieren Sie über eine kürzlich bekannt gewordene kritische Schwachstelle (CVE-2022-32158) im splunk Enterprise Deployment Server. Angreifer, die den „Universal Forwarder“ attackiert haben, können auch auf allen anderen Endpoints, die mit dem Deployment Server verbunden sind, beliebigen Code ausführen.

Betroffene Lösungen:

splunk Enterprise vor Version 9.0

Infoquellen/Referenzen:

[SPLUNK.com](https://www.splunk.com)

Unsere empfohlenen Maßnahmen dazu:

Folgen Sie den Hinweisen des Herstellers und führen Sie das entsprechende Upgrade auf Version 9.0 durch. Durch das Upgrade werden auch noch weitere wichtige, nicht kritische, Schwachstellen behoben.

Bei Fragen zu diesem Thema unterstützen wir Sie gerne unter support@bacher.at oder +43 1 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 customer,

with this newsletter we would like to inform you about a recently released vulnerability (CVE-2022-32158) rated with severity critical in splunk Enterprise deployment server. An attacker that compromised a Universal Forwarder endpoint could execute arbitrary code on all other Universal Forwarder endpoints subscribed to the deployment server.

Affected solutions:

Splunk Enterprise before version 9.0

Sources/references:

[SPLUNK.com](https://www.splunk.com)

Our recommendation:

Follow the given procedures from splunk and implement the upgrade to version 9.0 accordingly. This upgrade also resolves further non-critical, but important vulnerabilities.

We are at your disposal in case you need assistance or if you have questions. You can 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 on request to have this change implemented by one of our engineers.

Best regards

Bacher Systems Support Team