Advisory 2022-0259

OTRS: Mehrere Schwachstellen

Datum: 2022-02-07
Stand: 2022-02-07

Risiko gesamt

Angriffswahrscheinlichkeit: mittel-hoch
Potentielle Schadenshöhe: mittel

Plattformen

- Linux
- UNIX
- Windows

betroffene Produkte

- OTRS OTRS < 7.0.32
- OTRS OTRS < 8.0.19
- OTRS OTRS CustomContactFields < 8.0.12

Angriff

Ein entfernter, anonymer oder authentisierter Angreifer kann mehrere Schwachstellen in OTRS ausnutzen, um einen Cross-Site Scripting Angriff durchzuführen, vertrauliche Informationen offenzulegen und einen Denial of Service Zustand herzustellen.

Beschreibung

Das Open Ticket Request System (OTRS) ist ein Ticketsystem für Help-Desks.

CVE-2021-23368, CVE-2021-3803, CVE-2021-3807

In OTRS existieren mehrere Schwachstellen. Die Fehler bestehen aufgrund einer mehrfachen ineffizienten Komplexität regulärer Ausdrücke in nth.check und ansi-regex sowie eines Fehlers bei der Analyse von Source-Maps im Paket postcss. Ein entfernter anonymer Angreifer kann diese Schwachstelle ausnutzen, um einen Denial-of-Service-Zustand zu verursachen.

CVSSv2
AV:N/AC:L/Au:N/C:N/I:N/A:C/E:U/RL:OF/RC:ND
Base Score: 7.8
Temporal Score: 5.8
CVSSv3.1
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:X
Base Score: 7.5
Temporal Score: 6.5

CVE-2022-0473

In OTRS existiert eine Cross-Site Scripting Schwachstelle. HTML und Script-Eingaben werden in der "Fehlermeldung eines dynamischen Feldes" nicht ordnungsgemäß überprüft, bevor sie an den Benutzer zurückgegeben werden. Ein entfernter authentisierter Angreifer mit bestimmten Rechten kann durch Ausnutzung dieser Schwachstelle

CVSSv2
AV:N/AC:M/Au:S/C:P/I:P/A:N/E:U/RL:OF/RC:ND
Base Score: 4.9
Temporal Score: 3.6

beliebigen HTML- und Script-Code durch den Browser des Benutzers im Kontext der betroffenen Seite ausführen. Zur erfolgreichen Ausnutzung ist eine Benutzeraktion erforderlich.

CVSSv3.1
AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:L/A:N/E:U/RL:O/RC:X
Base Score: 3.5
Temporal Score: 3.1

CVE-2022-0474

Es existiert eine Schwachstelle in OTRS. Der Fehler besteht, wenn die Benachrichtigung so eingestellt ist, dass sie an jeden Empfänger einzeln gesendet wird. Ein entfernter authentisierter Angreifer mit bestimmten Rechten kann diese Schwachstelle ausnutzen, um vertrauliche Informationen offenzulegen. Zur erfolgreichen Ausnutzung ist eine Benutzeraktion erforderlich.

CVSSv2
AV:N/AC:M/Au:S/C:P/I:N/A:N/E:U/RL:OF/RC:ND
Base Score: 3.5
Temporal Score: 2.6

CVSSv3.1
AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N/E:U/RL:O/RC:X
Base Score: 2.4
Temporal Score: 2.1

Empfehlung

OTRS stellt Updates zur Verfügung. Bitte installieren Sie die aktuelle Version unter Berücksichtigung Ihrer Betriebssystemumgebung.
https://otrs.com/release-notes/otrs-security-advisory-2022-01/

OTRS stellt Updates zur Verfügung. Bitte installieren Sie die aktuelle Version unter Berücksichtigung Ihrer Betriebssystemumgebung.
https://otrs.com/release-notes/otrs-security-advisory-2022-02/

OTRS stellt Updates zur Verfügung. Bitte installieren Sie die aktuelle Version unter Berücksichtigung Ihrer Betriebssystemumgebung.
https://otrs.com/release-notes/otrs-security-advisory-2022-04/

Informationen

OTRS Security Advisory vom 2022-02-06
https://otrs.com/release-notes/otrs-security-advisory-2022-01/

OTRS Security Advisory vom 2022-02-06
https://otrs.com/release-notes/otrs-security-advisory-2022-02/

OTRS Security Advisory vom 2022-02-06
https://otrs.com/release-notes/otrs-security-advisory-2022-04/

Referenzen

CVE:CVE-2021-23368
CVE:CVE-2021-3803
CVE:CVE-2021-3807
CVE:CVE-2022-0473
CVE:CVE-2022-0474
OTRS:OSA-2022-01
OTRS:OSA-2022-02
OTRS:OSA-2022-04

Disclaimer

Die Angriffswahrscheinlichkeit wird durch den Nutzen Dritter (Motivation), den notwendigen Aufwand und die Möglichkeiten für einen Angriff bestimmt. Die Schadenshöhe wird durch den Aufwand zur Behebung des Schadens und die möglicherweise mittelbaren Auswirkungen des Schadens auf Geschäftsprozesse bestimmt. Es werden "worst case" Annahmen zugrunde gelegt.

Die veröffentlichten Informationen beruhen auf vertrauenswürdigen und zuverlässigen Quellen oder sind überprüft worden. Für die Vollständigkeit, Genauigkeit und inhaltliche Richtigkeit der Informationen wird nur insoweit eine Haftung übernommen, als grobe Fahrlässigkeit oder Vorsatz eine Haftung begründen. Jede darüber hinausgehende Haftung, insbesondere für mögliche Schäden, die durch den Gebrauch oder die Nichtverwertbarkeit der Informationen entstehen, wird ausgeschlossen.