Security Newsletter

2 July 2018

Subscribe to this newsletter

TicketMaster: Personal and Payment data breach, blaming Inbenta

Global entertainment ticketing service Ticketmaster has admitted that the company has suffered a security breach, warning customers that their personal and payment information may have been accessed by an unknown third-party.

A support chat tool, used to help dozens of major websites interact with customers, has been blamed for a security breach at Ticketmaster. One of the code libraries built by Silicon Valley-based tech firm Inbenta, which powers Ticketmaster's customer support agent, was sending payment data to an unknown third-party on customers who were buying tickets.

Inbenta chief executive Jordi Torras confirmed the security incident in a statement Thursday, but said that no other customers are at risk. "It has been confirmed that the source of the data breach was a single piece of JavaScript code, that was customized by Inbenta to meet Ticketmaster's particular requirements," said Torras.

The ticket-selling giant said Wednesday that international customers who bought tickets between September 2017 and June 23, 2018 -- when the malicious code was found -- may be affected. It's reported that as many as 40,000 UK-based customers who bought tickets between February 2018 and June 23, 2018 may also have been affected.

Read More

Official statement from Inbenta

Official statement from TicketMaster

Gentoo Linux distro hacked on GitHub, “all code considered compromised”

Downloaded anything from Gentoo's GitHub account yesterday? Consider those files compromised and dump them now—as an unknown group of hackers or an individual managed to gain access to the GitHub account of the Gentoo Linux distribution on Thursday and replaced the original source code with a malicious one.

Gentoo is a free open source Linux or FreeBSD-based distribution built using the Portage package management system that makes it more flexible, easier to maintain, and portable compared to other operating systems. In a security alert released on its website yesterday, developers of the Gentoo Linux distribution warned users not to use code from its GitHub account, as some "unknown individuals" had gained its control on 28 June at 20:20 UTC and "modified the content of repositories as well as pages there."

However, Gentoo assured its users that the incident did not affect any code hosted on the Gentoo's official website or the mirror download servers and that users would be fine as long as they are using rsync or webrsync from gentoo.org.

If you are the one who have downloaded Gentoo Linux images from GitHub instead of its official website, you are highly recommend to backup your content and reinstall the OS from scratch.

Read More

Official Statement from Gentoo

Cutting room floor

- For strong API security, you need a program not a piecemeal approach
- Facebook and Google accused of manipulating us with “dark patterns”
- PROPagate Code Injection Technique Detected in the Wild for the First Time
- Those Harder to Mitigate UPnP-Powered DDoS Attacks Are Becoming a Reality
- Hundreds of Hotels Affected by Data Breach at Hotel Booking Software Provider
- Free Thanatos Ransomware Decryption Tool Released
- Hotels, airlines and travel sites battle bot attacks
- ProtonMail DDoS Attacks Are a Case Study of What Happens When You Mock Attackers
- Least Privilege Access – Still at the Front Lines of Security
- How to access secrets across AWS accounts by attaching resource-based policies
- Betting giant BetVictor leaked a list of its own internal systems passwords
- Rampage and Guardian: RowHammer attack on Android and associated mitigation

#Tech and #Tools

- Open Source Security Trainings
- A collection of software, libraries, documents, books, resources about security.
- CTF Field Guide
- h1-search: Collect public disclosures for a HackerOne program
- Overcoming (some) Spectre browser mitigations
- Filezilla bundle: Malware behaviour?
- Reverse engineering AWS Lambda
- Playing with Relayed Credentials
- JSgen.py – bind and reverse shell JS code generator
- Streisand: Create your anti-censorship box (VPN, SSH, Tunneling...)

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us