

Malware & Threats ▾ Security Operations ▾ Security Architecture ▾ Risk Management ▾

DEVO

EBOOK CISO Strategy ▾ ICS/OT ▾ Funding/M&A ▾

Journey to the Autonomous SOC

Download Now



aws Available in AWS Marketplace

VULNERABILITIES

Vulnerability Provided Access to Toyota Supplier Management Network

Security researcher finds severe vulnerability providing system admin access to Toyota's global supplier management network.



By [Ionut Arghire](#)
February 7, 2023



A severe vulnerability in the web portal of Toyota's global supplier management network allowed a security researcher to gain access to sensitive information.

The issue was identified by US-based researcher Eaton Zveare in Toyota's Global Supplier Preparation Information Management System (GSPIMS), a web portal that provides Toyota employees and

TRENDING

The Effect of Cybersecurity Layoffs on Cybersecurity Recruitment

Zendesk Hacked After Employees Fall for Phishing Attack

Russia-Linked APT29 Uses New Malware in Embassy Attacks

Microsoft Urges Customers to Patch Exchange Servers

suppliers with access to ongoing projects, surveys, information on purchases, and more.

The issue, Zveare says, was related to the implementation of JWT (JSON Web Token) authentication and could allow access to any account to anyone using a valid email address.

Essentially, JWT is a session token that is typically generated when logging in to a website, and which is then used to authenticate the user to secure sections of the website or APIs.

What the researcher discovered was that Toyota's GSPIMS contained a function that would allow users to generate a JWT based on the provided email address, without requiring a password.

With corporate Toyota email addresses easy to guess – as they are using the format `firstname.lastname@toyota.com` – the researcher was able to guess an email address by searching the internet for Toyota employees that might be involved in the supply chain.

Next, Zveare used that email address to generate a valid JWT and used it [to access the GSPIMS](#). After some reconnaissance on the portal, he discovered an account with system administrator privileges and used the same method to access it.

The system admin account, the researcher says, provided access to everything on the portal, including information on over 14,000 user accounts, control over roles each account could have, details on all

Cyberattacks Target Websites of German Airports, Admin

Critical Vulnerability Impacts Over 120 Lexmark Printers

Meta Awards \$27,000 Bounty for 2FA Bypass Vulnerability

US Infiltrates Big Ransomware Gang: 'We Hacked the Hackers'

Daily Briefing Newsletter

Subscribe to the SecurityWeek Email Briefing to stay informed on the latest threats, trends, and technology, along with insightful columns from industry experts.

available projects, surveys, and various classified documents.

According to the researcher, the GSPIMS also provides the system admin with the option to log in as any of the available 14,000 users, to supervise their activities. The function that generates the JWT based on email address was apparently implemented to enable this option, but it also created a backdoor into the network.

An attacker with system admin access to GSPIMS could have created a rogue account for persistence, exfiltrated all available data, tampered with or deleted the data, and fetched the corporate email and roles of all 14,000 user accounts to target them in phishing attacks.

The researcher reported the vulnerability to Toyota on November 3, 2022. The car maker patched the issue shortly after.

Related: [Toyota Discloses Data Breach Impacting Source Code, Customer Email Addresses](#)

Related: [Toyota's Japan Production Halted Over Suspected Cyberattack](#)

Related: [Vulnerabilities Expose Lexus, Toyota Cars to Hacker Attacks](#)



WRITTEN BY

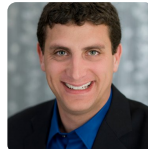
Ionut Arghire

Ionut Arghire is an international correspondent for SecurityWeek.

Business Email Address...

Subscribe

EXPERT INSIGHTS



Dealing With the Carcinization of Security

Varied viewpoints as related security concepts take on similar traits create substantial confusion among security teams trying to evaluate and purchase security technologies.

[Marc Solomon](#)



Stop, Collaborate and Listen: Disrupting Cybercrime Networks Requires Private-Public Cooperation

No one combatting cybercrime knows everything, but everyone in the battle has some intelligence to contribute to the larger knowledge base.

[Derek Manky](#)



How the Atomized Network Changed Enterprise Protection

Our networks have become atomized which, for starters, means they're highly dispersed. Not just in terms of the infrastructure – legacy, on-premises, hybrid, multi-cloud, and edge.

[Matt Wilson](#)



Mapping Threat Intelligence to the NIST Compliance Framework Part 2

How threat intelligence is critical when justifying budget for GRC personnel, and for