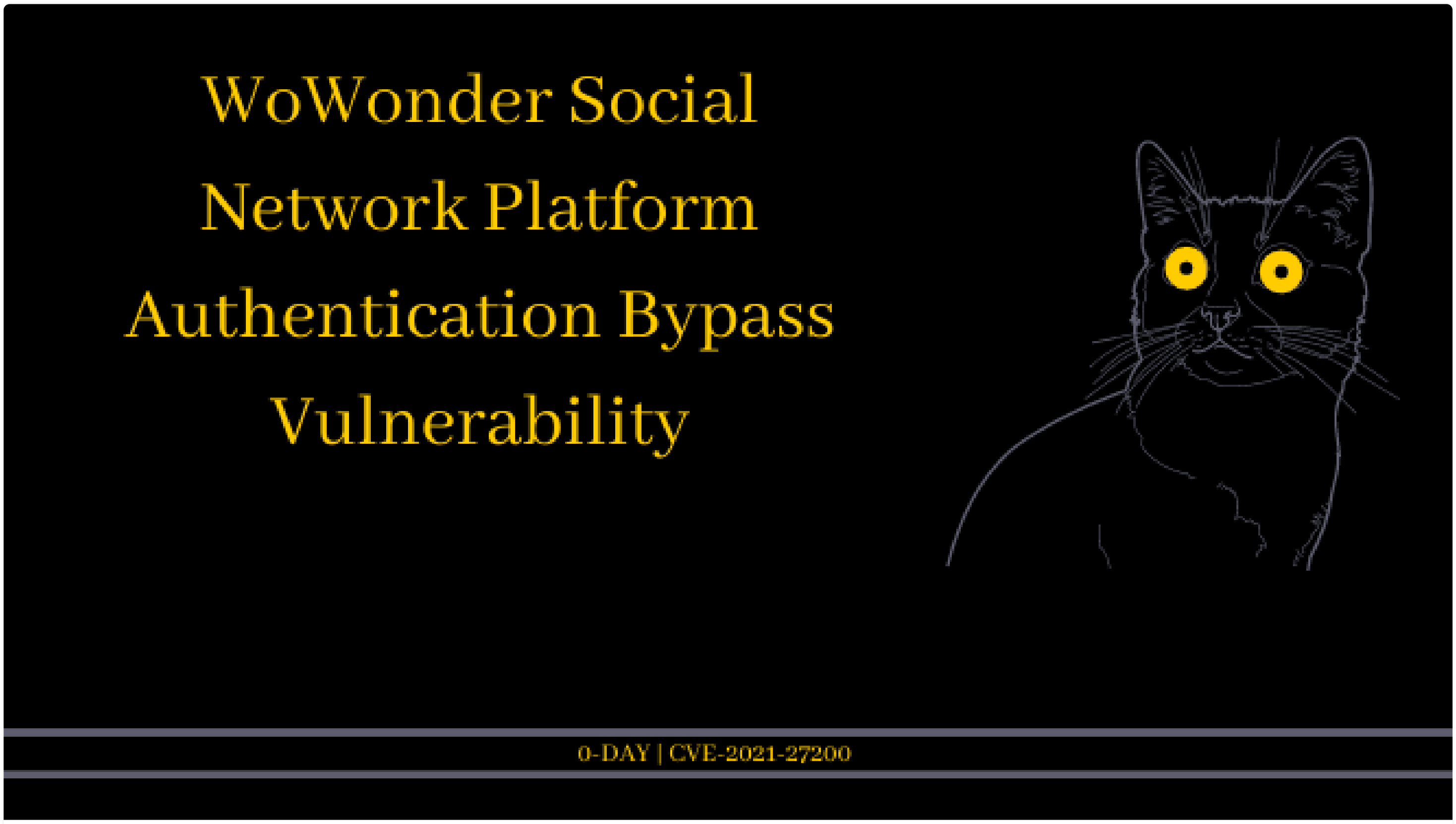
WoWonder Social Network Platform 0-day Authentication Bypass Vulnerability (CVE-2021-27200)

11/Jun/21


WoWonder Social Network Platform Authentication Bypass Vulnerability
0-DAY | CVE-2021-27200

For Companies Research

Wowonder is a web application software written using the PHP programming language that allows you to create your social networking platform. When the software is purchased through codecanyon, the source code will be included, and you will be able to run the software on your server. The application received an update and was released with a 3.1 version number after we notified the vulnerabilities that we found to the vendor.

As a result of our research on the Wowonder social network platform application, we detected an Authentication Bypass vulnerability caused by the "code" parameter in the password reset link.

Remote attackers can take over any account due to the weak cryptographic algorithm in recover.php file. The code parameter is easily predicted from the time of day.

If an attacker exploits this vulnerability, the attacker may access all accounts in the WoWonder application.

How Did We Detect Wowonder Social Network Platform Authentication Bypass Vulnerability?

As the Security For Everyone team, we regularly look for vulnerabilities in the software we have chosen to find 0-day. One of the software we chose was the Wowonder Social Network Platform web application, which serves as a social media platform. After deciding on the application that we are going to look for vulnerability, we performed the following steps in order:

- We decided to manually examine the source codes of the application purchased on Codecanyon after seeing that examining it with automatic source code analysis tools produced too many false positives.
- We determined that all requests are sent to the requests.php page by taking the function name as a parameter (requests.php?f=recover).
- We have seen that the "code" parameter in the password reset link is easily predicted from the time of day. The password reset code can be estimated by combining the password reset link time and the random value generated between 111 and 999.
- We discovered that the vulnerability could be triggered when we sent the estimated reset code to the password reset page.

What To Do?

After detecting the vulnerability, we reported the vulnerability to the Wowonder software team. Then, they fixed the vulnerability and updated the new version on Codecanyon. Downloading the current version and using it on your systems is recommended by the Security For Everyone team.

Sources

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-27200
- https://www.exploit-db.com/exploits/49989
- https://codecanyon.net/item/wowonder-the-ultimate-php-social-network-platform/13785302
- https://www.wowonder.com/

Search Keywords...

Tags Cloud

ANNOUNCEMENTS RESEARCH FOR COMPANIES FOR HOME USERS

Go Marketplace

Newsletter

✉ Your email:

Subscribe

Follow us

Company

- About
- Achievements
- Contact

Blog & Articles

- Blog
- Knowledge Base & Help

Newsletter

Your email:

Subscribe

Marketplace

- Marketplace
- Unlimited On-Demand
- Continuous Security
- Security Tools Collection
- Awareness Kit
- Advanced Support

Penetration Testing

- Penetration Testing Service
- Web Penetration Testing
- Mobile Penetration Testing
- IoT Penetration Testing
- Network Penetration Testing
- Request Pentest Service

Tool Collections

- Free Security Tools
- Subdomain Finder
- Allowed HTTP Methods
- DNS TXT Record Lookup
- SSL/TLS Supported Cipher
- DNS ANY Record Query
- TCP Full Port Scan

Useful Links

- Privacy Policy
- Terms of Use
- Changelog
- Service Status