SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

- Risk Management
- Compliance
- Privacy
- Supply Chain

- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - Network Security
  - Application Security
- Security Strategy
  - Risk Management
  - Security Architecture
  - Disaster Recovery
  - Training & Certification
  - Incident Response
- ICS/OT
- IoT Security

Home › Cloud Security

Google Patches Vulnerability in Cloud Endpoints Proxy

By Eduard Kovacs on October 01, 2021

A researcher has disclosed the details of a privilege escalation vulnerability he discovered in a Google Cloud component. The flaw was patched by Google in late August, but some users will need to manually update their systems to prevent potential exploitation.

The vulnerability was found by security researcher Imre Rad, who disclosed his findings last week on the Full Disclosure mailing list.

Rad found the vulnerability in Extensible Service Proxy (ESP), an open source, Nginx-based proxy that enables API management capabilities for JSON/REST or gRPC API services. Its features include authentication, monitoring and logging. ESP is a component of Google's Cloud Endpoints API management system, which is designed for securing, monitoring and analyzing APIs.

"If SSO is configured for an ESP fronted application where the identity provider is one of the popular ones (Google or Facebook) or an organization's internal IdP (e.g. Okta), then those API methods can be invoked by a malicious user assuming the identity of anyone," the researcher told *SecurityWeek*.

He noted that not all applications that use ESP are affected — applications based on PHP/Symfony are impacted, and possibly also some less popular frameworks. The researcher believes between 100 and 1,000 applications are affected, but he says this is a "gut feeling."

The vulnerability impacts ESP v1 and certain configurations — the researcher says ESP v2 is not affected. He also noted that some users will need to manually install the patches.

“Unlike with other services (e.g. MySQL instances of the Cloud SQL product), the ESP software is not operated by Google, so the burden of upgrade is on the customers. (Using ESP on AppEngine may be an exception, I think Google bumps the version there.) In line with this architecture, Google is not in the position to prevent abuse globally by implementing some magical server-side fix,” Rad explained.

Google has awarded a bug bounty for the vulnerability report, but the researcher did not want to disclose the exact amount — he said it was several thousand dollars.

“We rolled out a fix on August 31, 2021 to address this issue and ensure that all services are protected. We’re appreciative of the researcher’s work in identifying and reporting this vulnerability,” a Google spokesperson told *SecurityWeek*.

Google did not respond to follow-up questions regarding the number of impacted applications and users having to manually update the affected component.

Related: **Google Patches Privilege Escalation Vulnerability in Cloud Service**

Related: **Google Working on Patching GCP Vulnerability That Allows VM Takeover**

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’s security news reporter. Eduard holds a bachelor’s degree in industrial informatics and a master’s degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

Proposed Bill Would Require Organizations to Report Ransomware Payments
Google Patches Vulnerability in Cloud Endpoints Proxy
Hackers Can Exploit Apple AirTag Vulnerability to Lure Users to Malicious Sites
Contactless Payment Card Hack Affects Apple Pay, Visa
China Intensified Attacks on Major Afghan Telecom Firm as U.S. Finalized Withdrawal

Tags:
NEWS & INDUSTRY Cloud Security Vulnerabilities