SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy

Researcher Earns $10,000 for Yahoo! Mail Flaw

By Eduard Kovacs on January 19, 2016

A researcher has been awarded $10,000 for responsibly disclosing a stored cross-site scripting (XSS) vulnerability in the web version of the Yahoo! Mail service.

The flaw was discovered and reported in late December by Jouko Pynnönen of Finland-based software company Klikki Oy. The security hole allowed malicious actors to send out emails containing hidden JavaScript code that would get executed as soon as the victim read the attacker's message.

According to Pynnönen, an attacker could have exploited the vulnerability to compromise accounts, change their settings, and silently forward the victim's emails. The expert demonstrated how a malicious hacker could have sent the victim's inbox to an external website, and how they could have created an email virus that attached itself to all outgoing emails by silently adding malicious code to message signatures.

The problem was that the web version of Yahoo! Mail failed to properly filter potentially malicious code in HTML emails. Pynnönen noticed that the filters removed the value of boolean attributes, but the attribute itself and the equal sign following it were kept.

For example, inserting an image and using the "ismap" attribute, which defines an image with clickable areas, could have been used to execute arbitrary JavaScript with the following code:

```
<img ismap='xxx' itemtype='yyy style=width:100%;height:100%;position:fixe
d;left:0px;top:0px; onmouseover=alert(/XSS/)//'>
```

Yahoo! Mail would transform the code so that when the email was opened, the image was rendered across the entire size of the window, ensuring that the code in the "onmouseover" attribute got executed without user interaction:

```
<img ismap=itemtype=yyy style=width:100%;height:100%;position:fixed;left:
0px;top:0px; onmouseover=alert(/XSS/)//>
```

Pynnönen told *SecurityWeek* that Yahoo's filter did not remove the equal sign along with the value

of the attribute. Now that the vulnerability has been fixed, the equal sign is also removed, which makes the code look like this:

```
<img ismap itemtype='yyy style=width:100%;height:100%;position:fixed;left:0px;top:0px;
onmouseover=alert(/XSS/)//'>
```

“It wasn't specific to ismap. The same goes for a few other HTML attributes that work by being present or absent, e.g. <input type=checkbox checked> or <option selected>,” the researcher said via email. “In the corrected case above, the stuff after itemtype is no longer interpreted as separate style and onmouseover attributes, but the whole long string is the value of itemtype attribute. There is again no way to freely supply those ‘dangerous’ attributes.”

Yahoo! was informed about the vulnerability on December 26 and fixed it on January 6. The $10,000 bounty awarded to Pynnönen is one of the highest paid out by the company so far.

The expert reported two other bugs to Yahoo in December: a stored XSS in Flickr, for which he earned $500, and an issue that Yahoo closed after determining that it had been previously disclosed by someone else.

In July 2015, Yahoo reported paying out more than $1 million dollars since the launch of its bug bounty program in October 2013.

The stored XSS found by Pynnönen affected the web version of Yahoo! Mail, but not the mobile applications. In December, researcher Ibrahim Raafat reported finding a stored XSS in the mobile version of the Yahoo! Mail website. The bug identified by Raafat allowed an attacker to execute malicious code as soon as the victim opened their Yahoo! Mail account from the mobile version of the website.

Previous Columns by Eduard Kovacs:
Researcher Earns $10,000 for Yahoo! Mail Flaw
Ukraine Accuses Russia of Cyber Attack on Kiev Airport
Authentication Flaw Found in Advantech ICS Gateways
Encryption Flaw Used to Crack Cryptear Ransomware
Trustwave Sued by Casino Operator Over Breach Investigation

Tags:
NEWS & INDUSTRY Vulnerabilities

ALSO ON SECURITYWEEK PROVIDES INFORMATION SECURITY NEWS AND ANALYSIS. WHAT'S THIS?

Adobe Issues Emergency Patch For Flash Zero-Day Under Attack
1 comment • 22 days ago
Sean — Flash exploit du jour ou du heure?

World Bank Site Has Certificate Revoked After Hosting Phishing Page
3 comments • 2 months ago
Coal invoice — But but but, its Comodo, they get owned regularly. Its a security Company that can't even handle its own security. ;)

Second Database Exposing Voter Records Found Online
2 comments • 15 days ago
PY — Mainstream tech press is still clueless after all these years... Autistic cucks like Vickery troll Shodan for open mongodb's …

Vulnerable Joomla Servers See 16,000 Daily Attacks
3 comments • 22 days ago
Justin Gibbs — Agree with Alan it's not Joomla's fault, plus Joomla community provide some good security extensions to …

Subscribe Add Disqus to your site Add Disqus Add Privacy DISQUS

Most Recent Most Read

- Researcher Earns $10,000 for Yahoo! Mail Flaw
- Ukraine Accuses Russia of Cyber Attack on Kiev Airport
- LastPass Attack Could Result in Full Account Compromise
- Authentication Flaw Found in Advantech ICS Gateways
- Top Chinese University Hacked by IS Infiltrator: Reports
- Encryption Flaw Used to Crack Cryptear Ransomware
- Trustwave Sued by Casino Operator Over Breach Investigation
- Apple's Gatekeeper Bypassed Again
- Struggling With Privacy Tradeoffs in Digital Era
- Fifth Tinba Variant Targets Financial Entities in Asia Pacific

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

IT Security Newsletters
IT Security White Papers
Suits and Spooks
ICS Cyber Security Conference
CISO Forum
InfosecIsland.Com

Stay Intouch

Twitter
Facebook
LinkedIn Group
Cyber Weapon Discussion Group
RSS Feed
Submit Tip
Security Intelligence Group

About SecurityWeek

Team
Advertising
Events
Writing Opportunities
Feedback
Contact Us