SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

WRITE FOR US

- Subscribe (Free)
- Security White Papers
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Desktop Security
- 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

Kaspersky Patches Critical Vulnerability in Antivirus Products

By Eduard Kovacs on September 07, 2015

Kaspersky Lab has pushed out an update to address a serious antivirus vulnerability reported over the weekend by a Google security engineer.

Google's Tavis Ormandy reported on Saturday that he had discovered a flaw affecting the 2015 and 2016 versions of Kaspersky's antivirus products. A screenshot published by the expert shows a successful exploit against Kaspersky Anti-Virus, but it's unclear if Kaspersky Internet Security and other products were affected as well.

The researcher hasn't disclosed any details, but he says the issue is "as bad as it gets." The vulnerability appears to be a buffer overflow affecting the application's default configuration. Ormandy said his system exploit could have been used remotely with zero interaction.

The researcher reported his findings to Kaspersky and the security firm released a patch within 24 hours.

"We would like to thank Mr. Tavis Ormandy for reporting to us a buffer overflow vulnerability, which our specialists fixed within 24 hours of its disclosure. A fix has already been distributed via automatic updates to all our clients and customers," Kaspersky Lab told *SecurityWeek*.

"We're improving our mitigation strategies to prevent exploiting of inherent imperfections of our software in the future. For instance, we already use such technologies as Address Space Layout Randomization (ASLR) and Data Execution Prevention (DEP)," the security firm added. "Kaspersky Lab has always supported the assessment of our solutions by independent researchers. Their ongoing efforts help us to make our solutions stronger, more productive and more reliable."

Kaspersky Lab is not the only security firm whose products have been found to be vulnerable to hacker attacks. Researcher Kristian Erik Hermansen last week published details on what he claims to be a serious vulnerability affecting FireEye appliances. The expert says the flaw, which he reported to FireEye 18 months ago, can be exploited remotely to gain root file system access on affected appliances.

Hermansen claims to have identified several vulnerabilities in FireEye products, including command injection and login bypass bugs, which he now plans on selling.

"FireEye appliance, unauthorized remote root file system access. Oh cool, web server runs as root! Now that's excellent security from a _security_ vendor :) Why would you trust these people to have this device on your network?!?!?" Hermansen said.

FireEye said it only learned of the vulnerabilities on Monday morning.

"This morning, FireEye learned of four potential security issues in our products from Kristian Hermansen's public disclosure of them being available for purchase. We appreciate the efforts of security researchers like Kristian Hermansen and Ron Perris to find potential security issues and help us improve our products, but always encourage responsible disclosure," FireEye told *SecurityWeek*. "FireEye has a documented policy for researchers to responsibly disclose and inform us of potential security issues. We have reached out to the researchers regarding these potential security issues in order to quickly determine, and potentially remediate, any impacts to the security of our platform and our customers."

**Updated with statement from FireEye*

Previous Columns by Eduard Kovacs:

Kaspersky Patches Critical Vulnerability in Antivirus Products
PayPal Mobile Apps Plagued by Authentication Flaw: Researcher
Fiat Chrysler Recalls SUVs to Prevent Remote Hacking
Unpatched Firefox Flaws Exposed in Bugzilla Breach
Schneider Electric Patches PLC Flaws Disclosed at DEF CON

Tags:
NEWS & INDUSTRY Vulnerabilities

Subscribe to SecurityWeek

Most Recent Most Read

- Kaspersky Patches Critical Vulnerability in Antivirus Products
- PayPal Mobile Apps Plagued by Authentication Flaw: Researcher
- Fiat Chrysler Recalls SUVs to Prevent Remote Hacking
- Unpatched Firefox Flaws Exposed in Bugzilla Breach
- Snowden Attacks Russia Rights Curbs, Would Prefer to Go Home
- Schneider Electric Patches PLC Flaws Disclosed at DEF CON
- Security Professionals, Beware of Fake Recruiters on LinkedIn
- BlackBerry to Acquire Good Technology for $425 Million in Cash
- Cyber Intelligence: Competitive Intelligence By Any Other Name…
- Flaws in OrientDB Expose Databases to Remote Attacks

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