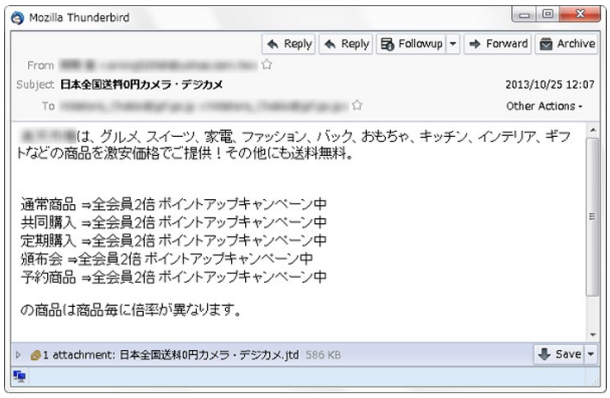
Japanese word processor 'Ichitaro' zero-day attack discovered in the wild

November 15, 2013 Mohit Kumar



Japanese most popular word processing software '*Ichitaro*' and Multiple Products are vulnerable to a zero day Remote Code Execution Flaw Vulnerability, allowing the execution of arbitrary code to compromise a user's system.

According to assigned *CVE-2013-5990*, malicious attacker is able to gain system access and execute arbitrary code with the privileges of a local user.

The vulnerability is caused due to an unspecified error when handling certain document files. "*We confirm the existence of vulnerabilities in some of our products.*" company blog says.

In a blog post, Antivirus Firm *Symantec* confirmed that in September 2013, they have discovered attacks in the wild attempting to exploit this vulnerability during, detected as *Trojan.Mdropper*, which is a variant of *Backdoor.Vidgrab*.

Researchers mentioned that *Backdoor.Vidgrab* variant was used as a payload for a watering hole attack exploiting the Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2013-3893), which was patched in October 2013.

According to them, it is reasonable to assume that the same malware group, or another group with close connections, is behind the attacks that utilized the Internet Explorer and Ichitaro vulnerabilities.

> *"Backdoor.Vidgrab is known to be used to target the Asia-Pacific region with government sectors being the primary targets."*

Vulnerable products:

- JustSystems Ichitaro 2010
- JustSystems Ichitaro 2011
- JustSystems Ichitaro 2011 Sou
- JustSystems Ichitaro 2012 Shou
- JustSystems Ichitaro 2013 Gen
- JustSystems Ichitaro 2013 Gen Trial
- JustSystems Ichitaro Government 2009
- JustSystems Ichitaro Government 2010
- JustSystems Ichitaro Government 6
- JustSystems Ichitaro Government 7
- JustSystems Ichitaro Government 2006
- JustSystems Ichitaro Government 2007
- JustSystems Ichitaro Government 2008
- JustSystems Ichitaro Portable with oreplug
- JustSystems Ichitaro Pro
- JustSystems Ichitaro Pro 2 Trial
- JustSystems Ichitaro Pro 2
- JustSystems Ichitaro Viewer

Popular This Week


Beware of 'Coronavirus Maps' – It's a malware infecting PCs to steal passwords


Warning — Unpatched Critical 'Wormable' Windows SMBv3 Flaw Disclosed


Critical Patch Released for 'Wormable' SMBv3 Vulnerability — Install It ASAP!


Microsoft Hijacks Necurs Botnet that Infected 9 Million PCs Worldwide


New Android Cookie-Stealing Malware Found Hijacking Facebook Accounts


Use This Ultimate Template to Plan and Monitor Your Cybersecurity Budgets


This Unpatchable Flaw Affects All Intel CPUs Released in Last 5 Years


9 Years of AMD Processors Vulnerable to 2 New Side-Channel Attacks

Attackers are distributing malware with spear phishing attack, as email attachments with the Ichitaro file extension *.jtd*, the files are actually .rtf or rich text format files. The files cannot be opened using Microsoft Word as they are designed to work only with Ichitaro.

> "*The attackers, possibly belonging to the APT12 group who may have also developed BackdoorVidgrab, are persistently targeting similar, if not the identical, targets by attempting to exploit Ichitaro.*" Symantec says.

A patch is available from the Ichitaro Web site to fix the vulnerability on the relevant products.

Have something to say about this article? Comment below or share it with us on Facebook, Twitter or our LinkedIn Group.

Latest Stories

Exclusive Offers